THE Open GROUP

Intrusion Attack and Response Workshop

Saving Private Data

A theatrical workshop written, directed, and produced by:

George Robert E. (Bob) Blakley III
Chief Scientist, Security & Privacy, IBM Tivoli Software

and:

Jane M. Hill
Barrister, Chambers of Benet Hytner Q.C. London

April 2003

The Open Group gratefully acknowledges the major contributions of the authors, producers, and directors of this workshop (Bob Blakley and Jane Hill), and the members of the cast (listed on Page 7) at the performance at The Open Group Conference in San Francisco, 3-7 February 2003.

The *Intrusion Attack and Response Workshop* was jointly sponsored by The Open Group Active Loss Prevention Initiative (ALPI) and the Security Forum.

Intrusion Attack and Response Workshop – Saving Private Data

ISBN No.: 1-931624-28-3

Document No.: W031

There is a video recording of the performance available on CD-ROM. Contact spd-video@opengroup.org.

Published by The Open Group, April 2003

Any comments relating to the material contained in this document may be submitted to i.dobson@opengroup.org.

Table of Contents

Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

The *Intrusion Attack and Response – Saving Private Data* workshop was conceived, written, and performed with the goal of making very serious points, in an entertaining way, about the nature and likely consequences to a business enterprise when it is the victim of an "incident".

Intrusion attacks on IT systems are becoming a significant hazard. The consequences to a business operation vary according to the nature of the business – enterprise, multinational, government, defense, and so on. This workshop elected to focus on a medium-sized enterprise providing IT services to its customers, and the issues that arise when such a business operation is attacked. It was designed in two Acts:

- Act 1: The discovery of the incident. As the intrusion attack is investigated, more and more damaging implications and serious consequences are revealed, and the company's Incident Response Plan (IRP) is tested (and found wanting) in a real "incident" situation.
- Act 2: The consequences of the responses, with uncomfortable lessons for many of the players. While the conclusion of the play is not too damaging, the issues raised show how the outcome could have been extremely damaging, to the extent of putting the company out of business by being unable to continue operating.

This White Paper presents a record of the workshop, including a checklist for managers whose responsibilities include their company's IRP. The whole script is provided with annotations highlighting the main issues raised and lessons to be learned. A video recording of the performance is also available on CD-ROM.

Overview

Goals

The objectives of this workshop were to present a plausible scenario for the actions a commercial enterprise might take when an IT system that a key part of their business operations depends upon unexpectedly goes down, and to bring out the likely consequences of those actions.

In doing so, the workshop raised the major issues that all IT-dependent businesses need to consider:

- The information security they should have
- The policies, Incident Response Plans (IRPs), and procedures they should have
- The drills they should rehearse to ensure their IRP is workable
- The need to regularly revise their policies, plans, and procedures to keep in step with their evolving business and maintain their preparedness

Rather than make these points in a slide presentation, the co-presenters decided to make them more interesting and real by bringing them out in a theatrical workshop, presenting a scenario staging detection of an intrusion attack on a corporate IT system, the corporation's responses to the attack, and the consequences of those responses.

Target audience

- Information Security Managers
- IT Operations Managers
- Business Risk Managers
- Corporate Counsel
- Corporate Communications/PR Managers
- Corporate Auditors
- Business Application Owners

The workshop

The workshop performance was directed in the same style as a "murder mystery" game, in which each actor was provided with scripted lines giving specific information or decisions that they must deliver at designated points in each scene.

Within this framework the actors were encouraged to *ad lib* additional dialogue and drama to add their own understanding and expertise into the character they were playing.

The two-Act performance took place at The Open Group Conference in San Francisco, 3-7 February 2003, as part of the Conference Plenary:

- Act I on the afternoon of February 3rd
- Act II on the morning of February 4th

Each Act comprised five Scenes, and lasted about 40 minutes. At the end of each Act there was a Q&A session with the audience, led by the producer/directors and actors, to highlight and clarify key issues.

Act I played out a sequence of response scenarios to a system unexpectedly going down and the subsequent discovery of an intrusion, illustrating the various priorities a business must reconcile when facing such situations, and bringing out the need for well-prepared and regularly updated response procedures to manage it well.

Act II used the outcomes from Act I to indicate the considerations that well-prepared response procedures need to include. It reviewed the business and legal consequences of the intrusion, liability to third parties, defense for any enforcement procedures (under data protection/privacy laws[1]), and steps to be taken to minimize potential losses, and to bring the hacker to justice (or not). It also considered whether and how much information about the intrusion and its consequences to disclose to clients, what law enforcement can demand regarding disclosure and even seizure of affected IT systems, sources of help using an ISAC or similar expert advisory organization, and the possible consequences of doing or not doing so.

[1] The concept of data protection is only really understood in the US under the title of “privacy laws”. This Saving Private Data workshop scenario was played out with only the application of what would be normal process under US state law. It would be played out differently in any other jurisdiction where data protection legislation exists.

Scenario

The cast

The cast comprised nine players providing the action.

Each member of the audience was encouraged to consider themselves as acting in the role of a Board Director of the attacked corporation and so bearing ultimate responsibility and liability to regulatory authorities, the law, and shareholders, for the consequences of the attack – including any financial and legal penalties, loss of ability to continue trading, and damage to reputation.

The players

Rocky Wardrop **StarCorp IT Operations Manager**	Walter Stahlecker Hewlett-Packard Company
Col. K. A. "Kelly" Rider (ret.) **StarCorp IT Security Manager**	Steven Jenkins NASA Jet Propulsion Laboratory
Lucinda Walls **StarCorp Order-Processing Operations Manager**	Sally Long The Open Group
Brenda Star **StarCorp CEO**	Jane Hill Viviale
David Auric **StarCorp Public Relations Officer**	Eliot Solomon Eliot M. Solomon Consulting
Brendan "Blowtorch" Boylan **Boylan, Boylan, Singh, Girardo** **(retained Counsel to Nebular Networks)**	Wes Kinnear Holme Roberts & Owen, LLP
Anna Williamson **StarCorp Corporate Counsel**	Ola Clinton Holme Roberts & Owen, LLP
Tim "the Terrier" Malone **Independent Daily Tabloid, Reporter**	John Mawhood Tarlo Lyons, London
Bailiff	David Lounsbury The Open Group
Johnny the Hacker	Allen Brown The Open Group
Board of Directors	The Audience

Act 1

In Scene 1, at 09.35 one day, StarCorp's Order-Processing Operations Manager (Lucinda Walls) gets a phone call to say the online order-processing application has gone down. Lucinda immediately reports this to StarCorp’s IT Operations Manager (Rocky Wardrop) and emphasizes the unusual nature of this failure which will not clear, and the urgency to restore service to StarCorp’s customers. The initial investigation indicates that it's a hacker attack. Getting the system back online is the company's highest priority. A SWOT (Strengths, Weaknesses, Opportunities, Threats) team headed by Rocky tries to identify and fix the problem. StarCorp CEO Brenda Star is at this very moment in line for a prestigious industry award and is determined that this incident will not torpedo her chances.

As the investigation proceeds, Col. Kelly Rider, StarCorp’s IT Security Manager, uncovers more evidence that indicates it’s a hacker attack, that it has come from “inside” – from Johnny’s machine in fact – and then that the attack extended to penetrate one of StarCorp’s customers – Nebular Networks – whose confidential data on a major government contract bid has been stolen.

As all this is revealed and StarCorp’s legal-eagle, Anna Williamson, notes the succession of possible repercussions, StarCorp’s PR Officer (David Auric) gets increasingly desperate over how he can contain the likely adverse publicity, while Lucinda keeps reminding everyone that StarCorp’s contractual eight hours to restore service is fast ticking away, and rails against the delays in restoring the order-processing service as a result of the time it is taking for Kelly’s “unworkable” Incident Response Plan (IRP) to complete.

Rocky eventually sides with Lucinda’s argument, and against strong objections from Kelly, rules that the lesser evil is to not complete the IRP and instead to restore the order-processing service just within the eight-hour limit. Amid the incensed feeling over Johnny’s treachery, Anna cautions that merciless prosecution may not be in StarCorp’s best interests. In the midst of all this, the local tabloid journalist Tim “the terrier” Malone drops in and sniffs a story that David finds it impossible to stop.

At the height of this angst, Johnny ventures in, and is arrested. Meanwhile, Anna and David have sent letters to their customers giving as little away as possible but ensuring they meet the letter of their obligations to inform. They have also written to Nebular Networks, again revealing as little as possible but nevertheless admitting that the StarCorp order-processing system has been used in an intrusion attack to obtain confidential data from Nebular Networks’ IT system.

Unsurprisingly, this stimulates Nebular Networks to accuse StarCorp of mis-management and send in their lawyer – Brendan “blowtorch” Boylan – who obtains a court writ and seizure order authorizing impounding of all

Nebular Networks' order-processing systems … a consequence being to prevent StarCorp from being able to continue service to all its customers. Anna desperately contacts the Court Judge involved to request an immediate stay of the order …

Act 2

In Scene 1, the StarCorp team take stock of their situation. Their corporate lawyer, Anna, lists several legal measures she has been able to take to help StarCorp to contain the impact of litigation in the event of this IT attack. She also notes that consequential damage arising from disclosure of a customer's confidential data can be included in Nebular Networks' claim for damages, and reminds them that an employer does have legal liabilities for the actions (good and bad) of their employees. StarCorp's IRP team discuss the arguments for and against going to court or settling out-of-court, and their lawyer explains the current prevailing attitudes of public prosecutors to criminal attacks on IT systems. StarCorp's managers also show themselves rather ineffective at keeping the press away from news that could damage their reputation.

In Scene 2, the consequences of StarCorp's response decisions in Act 1 are revealed, based on the claim received from their client Nebular Networks. This makes depressing news for StarCorp's managers. Nebular Networks claims that:

- StarCorp's system was not secure in the first place.
- StarCorp's security policies were deficient.
- StarCorp's procedures for screening and supervising employees were inadequate.
- Even if StarCorp's procedures and systems were adequate, they failed to follow their procedures and operate their IRP system properly.
- Specifically, StarCorp failed to follow their own IRP (which they claim was unworkable).

This Scene also discusses:

- What constitutes "reasonable security"
- The crucial role of properly recorded security audits
- The ineffectiveness of security policies (indeed, any policies) unless they are enforced
- The lack of security screening and supervision over an employee who was given wide access permissions in the IT system

None of this looks good for StarCorp if the case comes to court. Common practice is a partial defense, but should not be taken as a foolproof test. A company should also seek to use best reasonably available technology. Insurance can help but is not the full answer. StarCorp's managers also discuss how IT security breaches cost businesses billions of dollars worldwide. The Open Group Active Loss Prevention Initiative (ALPI) – including lawyers, insurers, and finance institutions – helps here.

In Scene 3, the IRP team assess more evidence and their exposure to Nebular Neworks' claim for damages. StarCorp's lawyer confirms the value of their IRP process to continue gathering all evidence, and cautions that when litigation starts, all relevant company information can be demanded by the claimant and must be disclosed – albeit possibly under non-disclosure – to the court, and if brought to trial is very likely to become public. Also audits of IT security are valuable in mitigating fault if they are conducted correctly. On the other hand, aborting their IRP by deciding to restore services to customers rather than complete the backups shows StarCorp up as having an "unworkable" IRP and putting profit before their customers' security, which will not look good in court or help their business reputation. Faced with all this, the StarCorp team begins discussing being able to settle out-of-court. Among the considerations that arise from this are that if they make an insurance claim to recover costs of a settlement, their insurers will bring in professional loss adjusters to conduct their own investigation, and their findings may also leak out and become public.

In Scene 4, Nebular Networks' lawyer, Brendan, conducts a legal deposition, illustrating how a cross-examination might proceed with StarCorp's manager responsible for their IT security. It is not that Kelly is a bad person, but it makes him look bad:

- Kelly is responsible for all StarCorp's IT security.
- Yet his organizational structure allowed an employee alone to do all this damage.
- And they deviated from their IRP.
- This deviation may have lost vital evidence.
- The reason why they deviated from the IRP is because it was in fact unworkable.
- Kelly has a battle in StarCorp to get their Security Plan prioritized.
- It looks to a jury as if StarCorp puts profit before their customers' security.
- StarCorp did not properly screen its key employees for their integrity.
- Yet they gave at least one employee wide powers to cause huge damage, and without adequate supervision.
- How can Kelly demonstrate that he completed a good security audit when he can't produce the Audit Report?

In Scene 5, StarCorp suggests to Nebular Networks that the evidence is that while StarCorp has not done everything right, Nebular Networks' case for large damages for consequential loss of a large government contract is very difficult to prove. The outcome is that they do agree an out-of-court settlement. This is typical of many IT security breaches, where the companies involved prefer to avoid the adverse publicity, damage to reputation, and legal costs of going to trial.

StarCorp's team is jubilant at containing the whole problem, as is their CEO, Brenda Star. Both Brenda and Rocky appreciate that StarCorp has significant things to put right in their organization, and this attitude bodes well for them succeeding in doing so.

Active Loss Prevention

Much of this *Saving Private Data* workshop concerns taking proactive measures to manage risk in a business whose operations rely on IT systems and the people who operate them.

This is the focus of The Open Group Active Loss Prevention Initiative (www.opengroup.org/alp).

The Initiative

The primary purpose of the Active Loss Prevention Initiative (ALPI) is to address the challenges relating to the proactive management of the full spectrum of information and eBusiness risks, backed by internationally accepted procedures and standards.

The Initiative takes a business view of what is required to deliver such risk management tools and techniques to the Internet-enabled business. In so doing, it manages the distinction between what is and is not delivered using the Internet. The Initiative is working towards a goal that will enable businesses to better manage the risks in their business environment.

The Initiative involves contributions from lawyers, insurers, auditors, and IT specialists. This primarily business view will be maintained throughout the projects managed under this Initiative.

Business risk

Enterprises and governments are increasingly dependent on extended, networked IT-enabled infrastructures. Many involve strategic assets, services, and funds with a direct impact on their customers. They seek the many benefits of eBusiness, yet manage risk in a piecemeal fashion, if at all, most often relying on technical solutions alone. Few of the checks and balances found in conventional business processes are present.

As a result, organizations around the world are exposed to largely unquantified or unmanaged risks whether from mishap or malicious attack. The consequences are potentially crippling. Only concerted global action can address these critical issues.

Active Loss Prevention – the way forward

The vision of Active Loss Prevention is the proactive management of the full spectrum of information and eBusiness risks, backed by internationally accepted procedures and standards:

- Drawing on proven models for managing fire risk in buildings
- Taking a strategic, enterprise-wide approach involving commercial, professional, human, and technology issues

- Proactive – anticipating risks, their impact and spread; and monitoring and responding to critical events
- For the first time, involving finance, audit, insurance, legal, and regulatory issues
- Will deliver the requirements for products and practices backed by global, consensus standards that can be tested, proven, certified, and supported by codes of practice and legislation

The Goal: Active Loss Prevention a reality for eBusiness

This Initiative brings together all stakeholders to develop and promote best practices and open standards. The work plan is designed to bring early benefits to participants whilst building the longer-term reality of Active Loss Prevention. It will address key legal and insurance issues at an early stage, providing a basis for assessing liabilities, insuring risks, and establishing legal underpinning for eBusiness for the first time.

Fast-forward

The Active Loss Prevention Initiative (ALPI) was launched in January 2002. It is strongly business-driven.

Traditional business and commerce has developed a supporting infrastructure over the course of centuries – checks, balances, and essential legal, insurance, and certification services. Business in the new, extended Internet-enabled enterprise has to establish this robust infrastructure in a much shorter timeframe.

With Active Loss Prevention added:

- Threats with crippling consequences are a fact-of-life in IT-enabled business. Executives now take informed decisions on these new risks and ensure systems are in place to actively manage them.
- Every eBusiness transaction, from mail to major contracts, is backed by internationally accepted verification related to the value and risk.
- No-one does business without it. Certified transactions have a clear assignment of liabilities and can be backed by new forms of insurance.

By achieving the vision of Active Loss Prevention, the infrastructure that enables eBusiness will become more closely aligned to the needs of business. It will also support the future demands for increased “trust” or confidence in it as the world economy relies further on eBusiness to sustain globalization programs and growth.

Issues

This section presents a more extended discussion on the major business, legal, technological, and process issues raised in this *Saving Private Data* workshop.

Resource allocation

1. IT budgets are often scaled to a certain percentage of income and security budgets are a percentage of that. What factors need to be taken into consideration when allocating funds/labor?
2. How much money/resources should have gone into implementing the Security Plan in *Saving Private Data*?
3. How would the technical answer be different from the legal answer?
4. How much profit is an organization legally expected to give up to cover downstream liability?

Organizational issues

1. The gap between the Security Plan, Kelly's general attitude, and the needs of the application owners, merits further exploration.
2. The workshop brought out some not untypical conflict between departmental managers who are not good teamworkers, and whose protective insular view of their role in the business overrides their respect for the total business of the company.
3. Why does Lucinda not appreciate that the company's security system – like its IRP – is the responsibility of all StarCorp’s managers, not just Kelly?
4. Do you have a records retention policy? Has it been reviewed by your legal staff?
5. Do you have a communications plan that describes how information about security concerns, risks, and incidents will be communicated to customers, partners, and the media? Has it been reviewed by senior management and your legal staff?

Legal issues

1. Does legal check your contracts?
2. Regardless of the regulatory situation, make sure you can live with the terms of the contract. Don’t ignore punitive clauses on the assumption they will never happen – they do and can be very damaging.

3. Consider how more warning of impending conflict between contractual and adverse publicity issues would have greatly relieved the problems.
4. Does StarCorp have reasonable protection for the data it holds about its customers? What does "reasonable" mean here?
5. Expand on the extent to which common practice is a partial defense, but should not be taken as a foolproof test. Include the case history and acceptability of a defense based on a company seeking to use best reasonably available technology.
6. Expand on the arguments for and against going to court or settling out-of-court.

Insurance issues

1. Does your insurance cover e-risk?
2. Do your operational practices meet the requirements of your insurance coverage?
3. Does your insurance cover liability for losses to third parties (business partners, customers, etc.) resulting from security incidents occurring in your system?
4. When was the last time you reviewed your insurance cover?
5. When reviewing your insurance cover, did you compare your coverage to your business processes and information systems?
6. Have you compared your insurance coverage with your business risk analysis? Did you verify and record this comparison using a formal analysis method?

Technical issues

1. IT Security Plans and IRPs need to be as effective as possible, yet also workable within the context of all the other dependent or related operations of the organization.
2. Reliability, Security, and Total Cost of Ownership (TCO) are the three mantras of information technology. Most businesses that depend on IT for their core operations have been in business for a few years and find their computing systems have evolved faster than their ability to plan that evolution such that it all works together. Multiple systems are usually the result, giving operational (data sharing), maintenance, and reliability problems that reduce business efficiency. Having multiple servers to back up as part of your IRP significantly increases your recovery/restoration of service time. We saw in *Saving Private Data* how the backup time exceeded the eight-hour customer service level agreement time allowed for restoration

of service.

3. One solution that StarCorp could consider is consolidating its IT systems to reduce the number of servers supporting their core business operations. While such migration will itself incur a significant up-front cost, the resulting operational efficiencies and increased systems reliability do represent a competitive differentiator to attract increased business customers, and reduced maintenance (licensing and staff) costs improve TCO and therefore increase profitability. Additionally – and most important here – recovery and restoration of service after an incident are significantly reduced.
4. When a business takes on additional IT risk, it should analyze the technical impacts and values attached to that additional risk, and take out additional security measures to mitigate that additional exposure to risk.
5. Have you performed a thorough risk analysis?
6. Have you updated your risk control processes and technologies taking the results of the analysis into account?
7. When was the last time you updated your risk analysis?

Business partner issues

How much should StarCorp have told their customers, especially Nebular Networks? And how soon? These are mostly legal issues. With increased networking and extending the enterprise business environment to include business partners and often significant suppliers and customers, the trend is towards more and more cross-enterprise activities. An example of a real problem a large business encountered from their extended enterprise is that one day they received an interesting call from a supercomputer vendor asking why they were attacking their sendmail port; it turned out that they had been infiltrated by hackers!

Publicity

The relationship between press, public statements, and corporate security is critical to the public perceptions of an organization's reputation, and therefore of its standing in their business sector. A good business reputation is hard to win, but very easy to damage.

How Active Loss Prevention helps

The Open Group vision of Active Loss Prevention is the proactive management of the full spectrum of information and eBusiness risks, backed by internationally accepted procedures and standards.

Drawing on proven models for managing fire risk in buildings, Active Loss Prevention:

- Takes a strategic, enterprise-wide approach involving commercial, professional, human, and technology issues
- Anticipates risks, their impact and spread, and monitors and responds to critical events
- Involves finance, audit, insurance, legal, and regulatory issues in one coherent activity
- Can deliver the requirements for products and practices that can then be backed by standards; these standards can in turn be supported by testing and certification schemes, and supported by codes of practice and legislation

Active Loss Prevention brings together all the stakeholders involved. It addresses the key legal and insurance issues, providing a basis for assessing liabilities, insuring risks, and establishing legal underpinning for eBusiness.

Checklist for Managers

This section provides a checklist for business managers, as an aid to validating the acceptance, practicability, and effectiveness of their IT Security Plan and Incident Response Plan (IRP).

Incident Response Plan (IRP)

1. Is your company IRP in place?
2. Have you included checks by your company auditors, legal advisors, and insurers, that the procedures, evidential collection steps, and insurance obligations and cover are appropriate and adequate?
3. When was the IRP last updated? It should be either every 12 months or whenever the company organization changes (including when a new person is appointed to a departmental manager position), whichever is the sooner.
4. When was the last time your IRP was tested?

Managerial responsibility

5. Does it assign clear authority and responsibility to designated departmental managers for:
    a. Awareness of the IRP?
    b. Regular training of their staff on implementing the IRP?
    c. Assignment of responsibilities for implementing the plan if an incident occurs?
6. Is that authority and responsibility backed-up by the overall company policy to make departmental managers responsible for awareness of and correct implementation of company policies within their department? The authority and responsibility for implementing company policies must be delegated from and demonstrably supported by the CEO, otherwise they will not carry effective force.
7. Do all affected departmental managers have a copy of the IRP?
8. Training and commitment: has the manager responsible for the IRP conducted a formal training and review meeting with all the other departmental managers present?
9. Have all the departmental managers signed off the IRP as accepted?
10. Have you clearly defined the responsibility of managers to supervise their employees, including ensuring that employees are not taking actions against the interests of the business?

Managerial delegation

11. Have all departmental managers appointed a designated chain of deputies who are assigned responsibility for responding to an incident in their absence? The IRP should not be put in jeopardy by the absense of a departmental manager (on company business, vacation, sickness, or for any other reason).

Personnel practices

12. How do you screen personnel upon employment?
13. Do you have processes or technologies which ensure that sensitive operations must be performed (or at least observed) by more than one employee, so that no single employee can violate policy without being observed?
14. Do you require employees with high privilege or access to sensitive systems or resources to indemnify the business for any breach of trust or policy; for example, by bonding?
15. How do you manage the lifecycle of accounts and permissions, in order to ensure that employees who no longer need access to systems or functions have that access disabled in a timely fashion?

Verify the IRP with business obligations

16. Do the operations in the IRP align with the service level agreements and similar contractual obligations to deliver operational services to your customers? For example, recovery procedures to gather evidence in an IRP must not conflict with contractual requirements for restoration of services to customers.

IRP audits

17. Has the latest version of the IRP been checked for effectiveness by conducting a practical drill exercise? Preparedness and effectiveness of staff in efficient response to IT incidents are significantly improved by holding exercises to convert the IRP into real incident response actions. The manager responsible for the IRP should operate IRP operational checks in the nature of an audit, in which:

    a. All IRP operations are tested for their effectiveness.

    b. Improvement points are identified.

    c. The IRP is updated to incorporate measures that implement these improvements.

    d. The improvements are tested by a further operational audit to verify their effectiveness.

   e. The IRP incorporating these audited and verified improvements is re-issued to all departmental managers responsible for implementing the IRP.

18. Have the results of the audit been shared with all departmental managers responsible for company policies, and explicitly for the IRP? This requires a further iteration of steps 4 through 6 above.

Leave nothing unverified

19. Has the manager responsible for the IRP verified genuine buy-in and commitment to the IRP from all managers responsible for its implementation? An IRP (like any plan) is of no real value if the managers you depend upon to implement it are allowed to consider it as merely a procedural nicety; a tick on a list of "things that should be in place if I'm asked"; yet another procedure to gather dust on an ever-lengthening shelf of policies and procedures that themselves intrude on your real day-job.

The CEO role is crucial

20. Does your CEO demonstrate their leadership and commitment to your IRP by regularly checking with managers that the IRP is updated, audits are held, and all the responsible managers are supportive of and aware/prepared/trained to execute any part of it? A company's culture is lead from the top: if the CEO demonstrates commitment to an effective IRP for the business and support for the manager responsible for the IRP, then this culture will permeate through all ranks.

It's people who make it work

21. Have you appointed the right person to implement your part in the IRP? A plan is only as good in its implementation as the people who operate it. Its overall implementation will only be as good as its weakest link, so make sure the links in your domain are sufficiently well-authorized and strong to withstand panic and pressure from perhaps more senior staff whose local concerns argue for you to deviate from what is a proven good plan.

Script and Commentary

The script of this workshop is annotated to highlight the key issues that it illustrates.

Act 1, Scene 1

When the lights come up, Lucinda Walls, StarCorp's Order-Processing Operations Manager, is sitting at a small table with a telephone, in a spotlight. The phone rings and she answers.

♦ ♦ ♦

Process:
The first alert that an incident may have occurred.

Lucinda (You'll be carrying on one side of a telephone conversation; the audience can't hear the other half.) Answer the telephone by saying: "Hello, Lucinda Walls. … The order-processing application is *down*? Since when?" Listen for a minute. Ask what happened, and how long it will be until it's back online. Listen for another minute. "What do you mean you don't KNOW?" "I want you to drop everything and get that application back online. Call me back in ten minutes!" Hang up.

Pick up the phone again and say: "Get me Rocky Wardrop please. It's urgent."

♦ ♦ ♦

Process:
Possible incident again promptly and correctly escalated.

Isn't it fortunate that all three of these senior managers are available! Who would Lucinda escalate to if Rocky was unavailable? ... or Rocky contact if Brenda was out?

At this point the spotlight will come up on Rocky Wardrop, StarCorp's IT Operations Manager, sitting at a conference table with a telephone.

Rocky The phone will ring. Answer it by saying: "Hello, Rocky Wardrop."

Lucinda Tell Rocky that the order-processing application is down and there's no estimated uptime.

Rocky Tell Lucinda that you'll call Brenda right away and get back to her. Hang up.

At this point the spotlight on Lucinda will go down.

♦ ♦ ♦

Rocky Pick up the phone and say: "Get me Brenda Star please. It's urgent."

Brenda (offstage) Answer the phone by saying: "Hello, Brenda Star."

Rocky "Brenda, it's Rocky Wardrop."

Process:
Typical – a conflicting agenda for Brenda to handle.
She delegates well!

Process:
Was this a scratch team dreamed up by Rocky – or is it an Incident Response Team team established in their IRP?

Do you have an IRP?

Process:
Good prioritization – a prompt response to a possible incident. Note it is not yet established that it actually is one.

Process:
Again, isn't it fortunate that all the senior managers involved in "incident response" are available? What are their delegation procedures if this was not the case? Have they all appointed "incident response" deputies?

Process:
Which of your managers are represented in your Incident Response Team?

Brenda "Rocky, can this wait? Tim Malone is interviewing me for the Daily Tabloid's Burlingame Businesswoman 2003 cover story."

Rocky "I'm afraid it's pretty urgent, Brenda. The order-processing-application is down and we don't know why, but it looks serious. What should I do?"

Brenda Control your tone carefully to make sure Tim doesn't figure out something is wrong – maybe give a little laugh as if to indicate: "Oh, is that all?" Then say: "Oh! Well why don't you put a team together and get closure? You have my full authority." Then (aside to Tim) say: "What, Tim? Oh, we've just learned that we've got another great opportunity!"

Rocky Tell Brenda you'll be gathering the team in the War Room as soon as you can get them together.

Brenda "Thanks very much, Rocky!" Hang up.

At this point, the spotlight on Rocky will go down. All other Scene 1 players (including Lucinda) will cross (in the dark – don't trip!) to the conference table.

♦ ♦ ♦

Lights up on the team gathered around the conference table.

Rocky Thank the team for assembling and call the meeting to order. Explain that the order-processing application is down, and that Brenda has asked you to resolve the situation with the help of everyone in the room. Mention that they are all to drop everything until this situation is sorted out.

Rocky Ask Lucinda to describe what's happened.

Lucinda Explain that the order-processing application is down, with no estimated uptime, and that this hasn't happened before. Emphasize that this isn't like previous outages which the staff have handled; in previous incidents service was restored quickly and easily. Explain that the order-processing application customer contract obligates StarCorp to restore service within eight hours.

Rocky Ask to see a copy of the contract.

Legal:
Aha – their Incident Response Team includes their legal advisor from the start; a very wise move for moderating the legal risks the incident may raise.

Anna *Introduce Prop 1 (contract with order-processing application customers).* "Here it is. I've highlighted a few key provisions. Under Section 17.23(b), we're permitted to take the order-processing application offline for up to eight hours to conduct system maintenance.

Of course, we're not conducting system maintenance here, so we can't rely on 17.23(b).

Instead we're operating under Subsection (c) which requires us to provide notice of an unscheduled interruption in service in a timely fashion.

Technical vs. Process:
First indication of conflict between operational and incident response.

The big issue is that if we don't restore the system within eight hours we risk incurring substantial financial liabilities. I'd like to begin working on the customer notice immediately."

David Ask whether the contract requires customers to keep the content of notifications confidential.

Legal vs. Process
Correctly worried about reputation and adverse publicity for the business.

Anna "No; the contract doesn't require customers to keep the notification letter confidential. Even if it did, we have hundreds of customers; it would be almost impossible to enforce something like that."

David "Well, then we'd better be damn careful what we put into these notifications, because it's going to show up in the Wall Street Journal and in all our competitors' marketing brochures. What were we thinking when we wrote this contract?"

Legal/Process:
Who fell short of a proper check on the terms of the contract here?

Does "legal" check your contracts?

Anna "David, I know you're upset, and you do have a point. This notice will be looked at very closely. We should assume customers will leak it to the press. A confidentiality clause wouldn't prevent leaks, but it could deter some. I'll look over our customer contracts when this is over and make sure we have confidentiality clauses in the future to cover situations like this."

David Tell Anna that you're sorry, and that you certainly did not mean to criticize her personally. Feel free to wink or grovel.

Rocky Ask what "a timely fashion" means in the contract.

Anna "The contract doesn't define "timely", and courts have interpreted timeliness clauses as a matter of interpretation and dependent on circumstances.

The more we delay, the more we'll need to do to justify the delay. If we can't justify it, we'll risk being held in violation of the terms of the contract.

I doubt we could get away with a delay of more than eight hours, given the penalty provisions."

Legal vs. Process:
More warning of impending conflict between contractual and adverse publicity issues.

Rocky Ask whether we know what's wrong.

Kelly Answer that you're running diagnostics because the incident looks suspicious, but we don't know what's wrong yet.

Technical:
Note the difference between investigation and response actions. Thorough investigation is vital to be sure that response actions are wise.

Rocky Ask Lucinda whether we haven't had outages before and restored service.

Lucinda Say that we have had outages, but this one is different and we don't know what's wrong. We aren't sure how long restoration is going to take because we've tried everything that's worked before and have not had success.

Rocky "It sounds like we have some trouble, then." Ask Kelly how soon you can have diagnostics done.

Kelly Reply: "Half an hour at the most; I'll get Johnny on it right away."

Rocky Tell Kelly it needs to be 20 minutes. Tell him you'll provide him with the network diagram and any assistance he needs.

Process:
Another example of unexpected situations – the press in the building – that needs careful handling.

Isn't it unwise to have a building security policy that escorts visitors (including the press) off the premises when their immediate business is done?

Rocky Tell Lucinda and Anna to start drafting the customer notification letters.

David Tell Rocky that you need to review the draft letters. Then tell everyone to remember that Tim Malone is in the building and that everyone (look at Lucinda and raise your voice when you say this) needs to be *very* careful not to allow Tim to overhear or see anything.

Rocky Tell the team to complete their assignments quickly and re-convene in half an hour.

♦ ♦ ♦

Lights down; Scene ends.

Act 1, Scene 2

When the lights come up Rocky and the team (except Kelly) are sitting around the conference table.

♦ ♦ ♦

Rocky Call the meeting to order.

Rocky *Introduce Prop 2 (the StarCorp network diagram).* Note that the order-processing application servers are indicated in red on the diagram.

Aside to players: The small (unlabelled) network segment in the lower right is the Nebular Networks system – this won't come up until Act 1, Scene 3, so don't talk about it!

♦ ♦ ♦

Kelly enters, a bit out of breath.

Kelly "Sorry I'm late; I can't find Johnny so I've had to supervise the diagnostics myself."

Rocky "No problem; have you got the diagnostics with you?"

Technical:
Thankfully Johnny's absense has not prevented sound investigation going ahead. What about the delays here if expertise on getting these diagnostics was not so well shared?

Kelly *Introduce Prop 3 (the order-processing application log for 2/3/2003).* "I've got the initial diagnostics, but we'll need some more detailed scans. Johnny hasn't shown up yet, but I've got the team working on it.

Lucinda (*casually*) "Johnny isn't in? That's not like him, is it? Where is he?"

Process:
First indication of more problems – where's good old dependable Johnny?

Kelly "I'm not sure. He hasn't called."

Rocky Ask Kelly what he thinks this log means.

Kelly Explain that the long sequence of mis-formatted orders in a short period of time looks very suspicious. Normally a mis-formatted order is the result of a data entry error by a customer's employee, and it takes a minute or more for the employee to correct the error and try again. In this log, many mis-formatted orders are coming in every second from the same address. Conclude that, though further investigation using system and intrusion logs will be necessary, you think this should be considered an attack.

♦ ♦ ♦

Technical:
First confirmation, backed up by investigation evidence, that an attack is the likely cause of the incident.

Lucinda When Kelly tells the team that he thinks your application is down because of an attack, ask him how come his security system didn't prevent this from happening. Feel free to act angry and betrayed.

Lucinda and Kelly Argue about whose fault the outage is. Kelly, feel free to point out that it was Lucinda who got your enhanced authentication system vetoed.

♦ ♦ ♦

Process:
Not untypical conflict between departmental managers who are not good teamworkers, and who's protective insular view of their role in the business overrides their respect for the total business of the company.

Rocky Let the argument go on for a little while. After a short interval, interrupt to end the argument and ask whether there's a process for dealing with attacks.

Kelly *Introduce Prop 4 (your IRP).* Explain that it's extremely important that the plan be followed to the letter, with the steps performed in the proper order. Also be sure to note the long hours of careful work your team put into making sure the plan is exactly right.

♦ ♦ ♦

Process:
IT security and incident response preparedness are important all the time, not just when an incident occurs.

Lucinda When Kelly introduces his complicated IRP, ask very pointedly whether this can all be done in eight hours. Point out that if it can't be done in eight hours, some steps are going to have to be left out, because you have a contract which promises to get the system back up in eight hours.

Lucinda and Kelly Argue about getting it right *versus* getting it done quickly.

Technical/Process:
The crucial issues Lucinda exposes here are that the IRP has not been audited to verify it is workable within the eight-hour contract time, and that she has no respect for Kelly's IRP.

How many other StarCorp managers share her hearty disrespect for Kelly's IRP – or even know what it says?

IRPs are important to the company, so should have buy-in from all managers.

Anna "My concern is whether we designed the plan to make sure we have admissible evidence in case our customers sue us.

Do we have a process for taking detailed written notes and preserving files and logs as we execute the plan?"

Technical/Legal:
Understanding what is "evidence" is vital. Did Kelly assume he knew it all? Shame – it seems that Anna too has not read the IRP. Did Kelly not consult legal to verify that his IRP preserves evidence?

Kelly "*Of course* the plan's been designed to preserve evidence. If people had read it, they'd know that."

Rocky When the discussion slows down, tell Kelly to start implementing the plan immediately but to keep Anna in the loop.

♦ ♦ ♦

Rocky Ask when the customers need to be told about what's happening, and what they need to be told.

Lucinda Make the point that the notifications need to go out *soon* and that they need to contain enough information to make the customers comfortable that StarCorp is on top of the problem and will fix it in compliance with the terms of the contract.

Technical:
The old enemy – time – is forcing the pace.

A good (audited) IRP, properly followed, will ensure effective use of time and assure wise response actions.

Anna "We've discussed this and decided we need to give notice within less than eight hours.

That only leaves us about three hours.

The letter needs to describe why the system is down, when we expect to resume service, and who our customers should contact for further information.

Please send me details for inclusion in the notice – what happened and what we've done to fix it.

Make sure everything you send me is accurate; if you can't verify it, don't send it to me.

Legal/Process:
Lessons here from Anna on how to handle legal liability in incident response communications.

We need to be careful not to speculate about the attacker's identity or motives.

Keep everything short and sweet, and get it to me within the next 30 minutes."

David Make sure that you're in the loop on these customer notifications, and make sure that no notifications go out until you're sure they won't damage StarCorp's reputation. Make some comment to the effect that: "We can't just have Lucinda writing random memos to the customers."

Process:
Another example of poor teamwork and lack of respect for the value each manager brings to the whole enterprise. Isn't the CEO responsible for fixing this problem?

Technical/Process:
Note that at this late stage in the eight-hour window they are still investigating and gathering evidence.

Lucinda Don't let David Auric get away with writing a watered-down letter to your customers and compounding the damage to StarCorp's reputation. Make sure you're on the team that writes the response to the customers!

Rocky Wait for the discussion to end, and tell Lucinda, David, and Anna to work on the text of the customer notifications.

♦ ♦ ♦

Rocky Tell the team to gather again in 30 minutes with Kelly's detailed diagnostics and the customer notification letter draft.

Kelly Tell the team that you'll get working on the additional diagnostics right away – but Johnny still hasn't shown up.

All "Where's Johnny?"

♦ ♦ ♦

Lights down; Scene ends.

Act 1, Scene 3

When the lights come up the team is assembled around the conference table again.

Rocky Call the meeting to order.

♦ ♦ ♦

Rocky Ask Kelly if the detailed diagnostics are done.

Kelly Answer that they are. *Introduce Prop 5 (detailed diagnostics).* Say you've just received them from the team and haven't had a chance to look at them yet.

The team looks at the diagnostics.

Process:
It's good that the whole Incident Response Team hears Kelly's diagnosis of the incident – binding them into a common cause.

Kelly Explain that "source" and "destination" identify the two ends of each connection. Point to the connections which delivered the malformed packets to the order-processing application. "You can tell which connections go to the order-processing application because the destination is x.36.22.1 or x.36.22.2. If you look at the "time" column, the ones we're looking for are the ones starting at 09:20:01 (that's the time the order-processing application log shows the first malformed packet arriving). Now let's see where the bad packets are coming from – the source address is x.36.25.36.

Uh-oh!"

Rocky Ask Kelly what's wrong.

Technical/Legal:
So the investigation finally reveals the attack was internal to StarCorp.

Kelly Explain that x.36.25.36 is an internal address – the attack came from one of our own systems!

Anna "What does that mean? Are you saying one of our employees did this?"

Kelly Explain that either one of StarCorp's employees is the attacker, or else someone's system has been infected with a Trojan Horse program.

♦ ♦ ♦

Process:
The pressure has again got to Lucinda – attacking Kelly for the company's security system, not just the IRP.

Why does she not appreciate that the company's security system – like its IRP – is the responsibility of all managers, not just Kelly?

Further evidence of a company culture problem.

Lucinda (Feel free to get upset.) Ask Kelly why his security system failed to prevent this.

Kelly Argue with Lucinda.

Rocky Cut off the argument and ask Anna whether this creates a legal problem for StarCorp.

Anna "If someone accessed customer data and we didn't use commercially reasonable efforts to protect the information, we might have a legal problem.

We certainly have a PR problem. We'll need a plan to manage the situation, David."

David "Damn straight!"

♦ ♦ ♦

Legal:
New legal liability issue – does StarCorp have reasonable protection for the data it holds about its customers?

During the previous discussion, Kelly has been looking through the diagnostics.

Kelly "I think there may be another problem."

Rocky Ask what it is.

Kelly “There’s also traffic originating at x.36.25.36 and going to e.112.57.5. Quite a lot of traffic, actually.”

Rocky “What’s e.112.57.5”?

Kelly Say it’s StarCorp’s link to Nebular Networks.

Rocky Ask what this means.

Technical/Legal: Even worse – the investigation indicates that StarCorp’s IT system has been used to attack a customer’s IT system.

Kelly Answer that there may also be an attack on Nebular Networks’ systems going on.

Rocky Order Kelly to go and investigate immediately and shut down the link if there’s a problem.

Kelly Call your team on the cell phone and order them to investigate.

♦ ♦ ♦

Rocky Ask Anna whether there are legal implications of an attack on Nebular Networks’ systems.

Anna “Yes; we have to deal with Nebular Networks as well as with our order-processing customers.

Legal: The legal liabilities a company faces if its IT system is used to obtain proprietary data from another company’s IT system.

The Nebular Networks contract was highly negotiated; that means that its terms are quite different from our standard customer arrangements. The Nebular Networks contract is very strict about unauthorized release of their data.

If Nebular Networks can prove that unauthorized parties got their proprietary data from us, we could be responsible for their direct financial losses.”

Rocky Ask if she’s familiar with the contract.

Legal/Process: Typical example of a business decision to accept additional risk to get new business. At least legal was consulted!

Anna “Yes; I’m familiar with it. In fact, I’ve got it here.”

Introduce Prop 6 (the Nebular Networks contract).

“I helped negotiate this contract; I advised at the time that some of its provisions are not in StarCorp’s best interest, but the business partner relations team were very anxious to close the deal and didn’t want to try to strike those provisions.

Technical:
Makes the point that when you take on additional risk you should also take additional security measures to mitigate that additional exposure.

Before we panic, though, we need to find out what happened, and what measures we took to protect Nebular Networks' systems.

I hope our protection measures were good, because there is a duty to protect Nebular Networks' assets in the contract as well as an obligation to notify them in the case that StarCorp becomes aware of an attack on their systems."

David Ask when Nebular Networks should be notified and what needs to be in the notification.

Anna "We're required to give them "prompt" notice."

David "What does that mean?"

Anna "In this case, it essentially means we have to notify them immediately.

Legal/Process:
Again, legal's lead on external notifications to customers is important in minimizing the company's exposure to reputation damage and possible future litigation from its customers.

We don't have any basis for delay, given the amount of information we already have about the attack. I'll draft the notice immediately."

David "What are you going to put into it? We need to preserve the Nebular Networks relationship; they're an important partner."

Anna "I'm going to stick to a brief description of the known facts; I'm not going to include anything the contract doesn't require."

♦♦♦

Lucinda Note that time is running out to restore service to the order-processing customers without triggering the penalties.

Process:
The clock is still ticking.

... Alas – the IRP was not audited to reveal how long backups take.

Now starts the real argument – to compromise the IRP or break the eight-hour customer service deadline.

Rocky Ask Kelly how the system backups and service restoration are going.

Kelly Answer that you can restore service now, but the system backups won't be finished for another three hours – past the deadline.

Lucinda Insist that service be restored.

Anna “Lucinda, we have written procedures.

An incomplete backup is a departure from those procedures.

If any data about the intrusion is missing from the backup, or if we destroy any evidence showing that it was a hacker attack, we could be in trouble.”

Rocky Ask Kelly if there isn’t something that can be done short of a full backup.

Kelly Insist that the full procedure should be followed; the IRP’s provisions are in place for good reasons.

Rocky Press the point.

Kelly Admit that you can do a quick but less complete backup (feel free to call it a “half-assed job” or some such thing), but you are sure it’s a bad idea.

Lucinda Insist on the quick backup.

Rocky Ask Anna what the risks are.

Anna “It’s very hard to be sure. If we have a plan and we depart from it, then we may be liable for failure to conform to our plan.

We need to make sure we take commercially reasonable steps to preserve evidence and identify losses.”

Process:
Well – when you’re between a rock and hard place, the top manager has to make the decision.

Did Rocky make the right one?

Rocky Order the quick backup, and restoration of service within the deadline.

Kelly Protest vigorously. After an argument with Rocky, grudgingly agree to do a quick-and-dirty backup, but tell Rocky that you are going to file a written protest.

Anna “Kelly, I don’t think it’s a good idea to write a letter like that.”

Kelly “I’m not going to do this without some record that I think it’s a bad idea.”

Anna “Kelly, a letter like this could look bad if it ever found its way into court. If you insist on writing it, please at least send me a copy. That way, we might be able to claim privilege.”

Process:
Sounds like the company culture is persuading Kelly to cover himself; he obviously distrusts his executive management. Whose failing is this?

Kelly "I'll be glad to send a copy to whoever you want."

Rocky Ask Anna and David to work on a notification letter addressed to Nebular Networks. Ask everyone to reconvene in 30 minutes.

♦ ♦ ♦

Lights down; Scene ends.

Act 1, Scene 4

When the lights come up, the team is assembled around the conference table again.

Rocky Call the meeting to order.

Lucinda Your cell phone rings. Answer and listen. Look at your watch. Tell Rocky that the application is back online.

Technical/Legal:
Like the true security professional he is, Kelly perseveres as best he can to preserve evidence that may be useful in any future litigation.

♦ ♦ ♦

Rocky Ask Kelly if the system image is done.

Kelly "We've backed up the machine which executed the attack – it was Johnny's. We've also backed up one of the two replicas of the order-processing application server, and the machine at our end of the Nebular Networks link. We've also backed up as many other machines as we could in the time available, but we had to stop before we finished the other order-processing replica, some of the enterprise application servers, and about half of our user workstations. I'm continuing the backups of the rest of the systems on a new CD, so we'll be able to tell which ones were backed up before we restored service and which ones we didn't get to until later. Here's the manifest of the backup we finished before we restored service." *Introduce Prop 7 (the incomplete system image).*

Process:
A snipe from Lucinda – bu t a key point on organizational exposure.

Most attacks do originate from an inside job.

How do you protect against this?

Lucinda "So one of *your* people did this? I guess we know why he's not at work, don't we Kelly?"

Rocky Ask Lucinda whether the order-processing customers were back online in time to beat the deadline.

Process:
Well done Rocky – at least StarCorp has succeeded in restoring service within the contractual time limit. To have failed here as well as compromised their IRP would have been very sad.

Lucinda Answer that they are, but we just barely made it in time. Worry that some customers may dispute our timing and try to recover penalties anyway. Complain that the IRP takes too long.

Kelly Point out that you have a timestamp in the log indicating when service was turned back on. Point out furthermore that if you had been allowed to improve the security of StarCorp's systems last year, it wouldn't have been necessary to use the IRP.

♦ ♦ ♦

Process:
Another example of needing a company culture that takes its system security seriously on a continuous basis.

Rocky Ask Kelly what happened on the Nebular Networks link.

Kelly Answer that it's bad news. Potentially very bad. It looks like Johnny penetrated Nebular Networks' file server and stole their response to the State Government for the new Power Trading network bid. It looks like he got everything – costing estimates, time and materials estimates, parts manifests, subcontractor identities and bids – lots of very proprietary information.

Anna "Where's Johnny?"

Technical/Legal:
Still continuing important investigation revealing more potential legal liability for proprietary data stolen using a company's IT facilities.

Kelly Answer that he doesn't seem to be on the premises, but they've found two tickets to Rio de Janeiro on his desk. It looks pretty bad.

Rocky Ask Anna how bad it is.

Anna "It's very serious. The Nebular Networks contract requires us to protect Nebular's assets.

That means we need to protect Nebular's data against insiders as well as outsiders.

If we didn't screen Johnny properly when we hired him, or if we failed to supervise him, or if we gave him unwarranted access, we could be liable for substantial damages.

Even if everything was in order, Johnny was our employee and was using our equipment for the attack. That alone could expose us to liability for his actions."

Rocky Ask Anna what's in the draft of the notification to Nebular Networks.

Legal:
What is legally important to include and exclude in company notifications to customers.

Anna "I've stuck to the facts and the timeline.

I didn't identify the hacker, because the contract doesn't require us to do so.

If we name Johnny and identify him as an employee, Nebular will definitely use it against us.

If we're somehow mistaken about Johnny's actions or the extent of his involvement and we name him in the notice, he could sue us."

David Ask whether Nebular Networks is required to keep the contents of the letter confidential.

Legal:
Once information leaves your company it is rarely in your control to prevent wider public disclosure.

Anna "No; there's nothing in the contract which requires confidentiality.

Nebular has shareholders to answer to, and they'll want to explain to them what happened.

I'll try to negotiate a non-disclosure agreement to cover the notification letter, but under the circumstances, I'd be very surprised if they'll sign it."

David (Feel free to get upset.) "Dammit, why don't we just take out an ad in the newspaper?"

♦ ♦ ♦

Process:
Again, company policy should be to escort visitors (especially the press) on, around, and off your premises.

At this point there's a loud knock on the conference room door. Tim Malone enters.

Tim "Hey, Lucinda – how are you doing? And David – it's been a long time! Listen, a little birdie whispered in my ear that you guys might be having a problem. Could I ask you some questions?"

Process:
A reminder to treat the press warily – they rarely act to keep your company information secret or to serve your purposes, so be very careful when talking to them.

Rocky "Uh, Tim, we're in the middle of a meeting right now – can you schedule an interview through David's office?"

Tim "Why all the formality, David? Is the problem that urgent?"

David "It's OK Rocky; I'm always happy to talk to Tim. Listen, Tim, how about if you head over to my office. Tell Sandy that I'll be right over for an interview and grab yourself a cup of coffee. I'll be there in about five minutes – I've just got to finish up the last detail on a press release with Rocky here."

Tim leaves reluctantly.

♦ ♦ ♦

David "What do you want me to say?"

Process:
Good practice is to agree internally (preferably while not under pressure) what to tell and not tell the press, or customers, as David does here with Rocky.

Rocky Tell David to say as little as possible, but make sure it's all true. Tell him to admit a system outage if he's pressed, and tell him that it's OK to say that we're investigating to see whether it's a system failure or a security incident. Tell him to keep the interview short and get back as soon as possible.

David leaves the room. Spotlight goes down on the conference table and comes up on Tim and David, both standing.

♦ ♦ ♦

Tim Tell David that everyone looks pretty worried – it must be pretty bad.

David Ask what the "it" he's referring to is.

Tim Say you've heard that a hacker has taken StarCorp's data center down and all the customers are offline.

David Say you're not sure where he gets his rumors, but the data center is not down, and most customers are having no problems. There's been an application outage, and StarCorp is working to restore service just as it always does in these cases.

Tim Ask if this is just like the rest of these cases, or if there's something more sinister going on. After all, the hackers are getting very clever these days, and it's no disgrace to get hit.

David Say that StarCorp is aware of the threat of hackers and takes it seriously, and say that you are of course investigating to determine the source of the outage.

Tim Ask if that means you don't know if it's a hacker.

David Say you're investigating to determine the source of the outage.

Tim Ask if that means you think it *is* a hacker.

Process:
Tim demonstrates that a mere sniff of an event is enough for a keen pressman to create a plausible, and usually exaggerated story. That's what sells newspapers!

The lesson is don't invite them near if you want to avoid this.

David Say "Come on Tim, give me a break! I just *told* you we're investigating …"

Tim "You'll give me a call just as soon as you know, won't you, David?"

David Say you don't really think it's news, but you'll send over a press release if one is issued, and Tim's free to call back at any time.

Spotlight down on Tim and David, back up on the team around the conference table.

♦ ♦ ♦

Rocky Ask Lucinda whether the notification letter was sent to the order-processing application customers in a timely fashion.

Lucinda Answer that it was. *Introduce Prop 8 (notification of StarCorp's order-processing application outage).*

Rocky Direct Anna to work urgently on the notification letter to Nebular Networks.

Process/Legal:
It seems the full extent of the investigation is now completed, and the outcomes are now being drawn together, to assess as a whole and form a more considered response in line with what remains intact in the IRP.

Tell everyone to reconvene when it's done, and think about what will go into the team's report to Brenda.

♦ ♦ ♦

Lights down; Scene ends.

Act 1, Scene 5

When the lights come up the team is assembled around the conference table again.

Rocky Call the meeting to order.

♦ ♦ ♦

Process:
As we could have predicted, the press coverage has done what StarCorp least wanted.

David *Introduce Prop 9 (Tim Malone's story).* Complain loudly that Tim wrote down speculations without checking his facts, and he even got your title wrong. And he quoted you so far out of context you don't even recognize yourself. Get mad.

Lucinda Ask David whether he'll stop badgering you about interviews now that he's screwed one up.

Process:
Lucinda's observations again reveal she's not a good teamplayer in StarCorp's organization.

David Tell Lucinda to grow up.

Anna "Unfortunately, Tim's speculations were pretty close to the mark.

I'm sending the notice to Nebular Networks immediately. Here's the text."

Introduce Prop 10 (notification of system intrusion).

Rocky Ask Anna what liabilities the notification letter will create, and which ones it will avoid.

Anna "Sending the letter will protect us against a breach of contract claim based on failure to provide prompt notice.

Legal:
More points that demonstrate why legal considerations are vital when a company is forming external communications to incidents – and not just ones that involve IT systems.

Nebular Networks might take the letter as an admission of liability for serving as the source of the attack.

I've tried to be very careful about spelling out the actions we took to detect and stop the attack.

The letter is designed to show that we met our obligation to protect Nebular's assets, but we'll have to see if it works."

Rocky Tell Anna to send the letter.

♦ ♦ ♦

Rocky Tell the team that Brenda has asked for a report on the incident. Ask what it should include.

Kelly Say you can provide the facts and a timeline of the incident, as well as a list of what was taken from Nebular Networks. Say you'll also provide a report of how much of your staff's time was taken up in the response.

Lucinda Say you can summarize the losses the order-processing application customers are claiming, and a summary of the time and labor your organization used in responding to the incident.

Process:
These three managers' responses to Rocky's request are the first clear indication that these managers ***can*** *operate as a cohesive team supporting the corporate needs of the company.*

David Say you'll summarize communications to third parties, including the press. Be sure to note that you'll provide an *accurate* transcript of the interview with Tim Malone. Ask whether StarCorp needs to issue a press release to correct Tim's story.

Anna "At the moment, any further discussion of the incident with the press doesn't seem like a good idea."

David Complain that this will leave you looking like an idiot.

Lucinda Say you don't see why that's a problem.

Process:
Whoops – but Lucinda hasn't forgotten how to leave out the teamplayer thing ...

Anna "David, I know it's difficult, but you didn't do anything wrong. Publishing a denial, or anything that looks defensive, is just going to make Tim want to come back for more and keep the story alive.

I'm afraid the best thing to do is wait. Things may not turn out too badly. Don't worry – we'll get through it."

Kelly *Your cell phone rings.*

Answer, listen, and then (in an excited tone) tell the team that Johnny is in the building.

♦ ♦ ♦

Bailiff (*offstage*) Shout: "Come back here, you! Stop and put your hands up!"

At this point, the Bailiff enters, crossing the stage, leading Johnny in handcuffs. Tim Malone follows with a camera, flash bulbs flashing.

Process/Legal:
The originator of the attack is apprehended.

The question now is what to do with him.

Bailiff "Thought you could run, did you?"

Johnny "You got me, copper, but you'll never make it stick."

Kelly "I'm afraid we will, Johnny."

The Bailiff leads Johnny offstage, with Tim following behind.

Johnny (as you're dragged away) Shout: "*Remember Kevin*!"

Legal:
Kevin Metnick is arguably the most celebrated case to date of a computer hacker.

♦ ♦ ♦

Rocky Ask Anna if StarCorp should press charges against Johnny.

Anna "I'm not sure. The District Attorney probably won't bring charges unless we can provide good evidence to support them. If we have to introduce our backup as evidence, it'll make our security look bad. And that would make our public relations problem even worse."

Legal/Process:
The decision for a company over whether or not to prosecute, or even to reveal an intrusion attack has happened, is a difficult one. Currently, considerations over damaging publicity adversely affecting business reputation and customer confidence often outweigh the natural desire to prosecute the offender.

Kelly Complain loudly that we should damn sure sue after all the damage that traitor Johnny did and all the work we had to do to clean up after him.

Rocky Tell Kelly that it doesn't need to be decided right away. Ask Anna to look into the option of a civil suit, and include it in the report to Brenda.

Anna "I will. I'll also summarize the liabilities we could face because of this incident."

♦ ♦ ♦

A loud hammering is heard at the door.

Bailiff (*offstage*) Shout: "Open up! Police! We have a warrant!"

Anna Cross the stage to open the door.

Legal:
An aggrieved customer will usually seek redress for disclosure of their proprietary or confidential data. Obtaining a writ is inexpensive!

How far can the legal actions extend?

Bailiff "I'm here to serve a warrant on StarCorp." *Introduce Prop 11 (the writ).* "This is Mr. Boylan from Nebular Networks. Please do what he says."

Anna "Hello, Mr. Boylan. I'm Anna Williamson, StarCorp General Counsel. Your reputation precedes you. What seems to be the problem?"

Brendan "The problem, Miss Williamson, seems to be that your employees have stolen my client's property. Please ask all of your personnel to move away from their computers immediately."

Anna "Don't be ridiculous; that would completely disrupt StarCorp's operations."

Brendan "It's not only possible, it's going to happen and it's going to happen now. I have a seizure order which allows me to remove from the premises all computer systems involved in the attack."

Anna *Read the order for a minute.*

"Well, Mr. Boylan, it looks like you have your paperwork in order. It's too bad you're mistaken about what actually took place."

Turn to Rocky.

"This seems to be a valid order, Rocky."

Turn back to Brendan.

"Mr Boylan, we'll move everyone away from the computers, but won't turn any of them off, and we won't allow any seizure until I've confirmed the order with Judge Landis and filed a motion to quash."

Brendan Tell Anna that you'll see about that and order the Bailiff to begin seizing computers immediately.

Anna Get out your cell phone, and make a call. "Judge Landis, please. It's urgent."

♦ ♦ ♦

Lights down; Scene ends. Pause briefly. House lights up. Act 1 ends. Cast wait for applause, then exit.

Legal:
The possible legal action varies according to the jurisdiction that applies in the country where the offense occurred.

This workshop was performed in the USA and so is set in the context of a USA jurisdiction.

However, it can extend to impounding the systems involved. If these are needed to operate your business, ***such action could stop your ability to continue trading.***

It could happen!

What risk management measures and insurance cover is appropriate to your business for a situation like this?

Act 2, Scene 1

Lights up; the team are assembled around the conference table.

♦ ♦ ♦

Rocky Welcome everyone. "Anna, what's our status on the search and seizure order?"

Anna "I finally reached Judge Landis – we had a short hearing this morning.

The bottom line is that there's no way we can resist giving Nebular Networks a copy of all the relevant parts of our system.

Legal:
Here are several legal measures that help to contain the impact of litigation in the event of an IT attack.

No computers are going to be seized, but we need to hand over the backups we've already made.

We've persuaded the judge to order Nebular to put up a bond as security so that if their actions turn out to be unjustified, they will have to pay us for any business losses arising from the order."

Rocky "That's the good news, now where do we stand with the writ?"

Anna "Nebular Networks are suing for damages arising from Johnny's actions. Nebular is claiming that Johnny sold the stolen information to one of their competitors.

Legal:
Consequential damage arising from disclosure of a customer's confidential data can be included in their claim for damages.

The government has just announced the Power Trading network contract award, and Nebular *did* lose the contract to a competitor.

David "Can they sue *us* for that? I know he's an employee, but when it's fraud like this – how could we have seen this coming?"

Anna "It's true that we aren't responsible for everything Johnny does, but we do have legal responsibilities.

Legal:
An employer has responsibilities for the actions (good and bad) of their employees.

We have a duty to ensure trustworthiness of employees, supervision, systems to protect against dishonest actions, and so on …

Nebular will claim that we haven't met those responsibilities."

David “That still doesn’t seem right. I can understand an organization being responsible for an employee in the normal course of things, but this?”

Anna “We’ll use that argument in our defense.”

♦ ♦ ♦

David “If this goes to court, what happens to our reputation? Presumably all the details will show up in the Daily Tabloid.”

Legal/Process:
The arguments for and against going to court or settling out-of-court.

Anna “That’s very likely – the press will love this, but there’s not a lot we can do about that.”

David: “So what do we do? Just pay up? That’s extortion – but we can’t afford for this to get out.”

Rocky “I’ve already talked to Brenda. She thinks we need to extract ourselves from this mess fast. What are our chances? Can we make them an offer to settle?”

Anna “It’s a very large claim – Nebular says the information Johnny leaked lost them the government contract.

Of course, they’re assuming they would have won the contract if this hadn’t happened.

We could try making an offer just to see if they’ll drop the action, but they have got us over a barrel – they know we can’t afford the publicity.”

Legal:
A public prosecutor’s position over whether to criminally prosecute hackers seems to vary according to national jurisdiction and the severity of the effects of the computer crime.

David “You can say that again.”

♦ ♦ ♦

Lucinda “What about Johnny – surely we are going to put him behind bars?”

Anna “I have talked to the DA’s office – in principle they are prepared to prosecute; they regard this sort of offense as being extremely serious.”

Lucinda "What does that mean?"

Anna "Well, computer crime is a big issue at the moment, and can carry some pretty severe sentences – also, in this case, there is the breach of trust element. Johnny was an employee in a position of trust – Judges take a dim view of that."

Process:
David shows he's not above getting back at his colleague Lucinda – another instance that corporate culture needs to quell.

Lucinda "OK, so let's go ahead and prosecute the … (insert suitable epithet)."

Anna "If charges are pressed, the DA will need us to co-operate and provide evidence. It will also mean some of you giving evidence in court."

Lucinda "Fine by me – I have plenty to say."

David (a*side*) "That's what I'm worried about!"

♦ ♦ ♦

Process:
How did anyone (Building Security personnel) let the press in unescorted and unwanted again? ... and after all the damage they've caused you over this incident!

Whose policy needs enforcing here?

Enter Tim Malone, with flash bulbs flashing.

Tim "Hey guys, any comment on the latest …"

David "Sorry, Tim – not right now."

David tries to usher Tim out. Tim needs to be stubborn – there's a good story here. Stand your ground – fire off as many questions as you can to the various characters, before David manhandles you out of the door.

Tim "So will Johnny be prosecuted? Who else was involved? Was any other data compromised? What about customers' personal data? Does this breach your privacy policy? Are people going to get fired? Are you expecting any more lawsuits?

Process:
These are all great news points ...

... as Rocky readily admits.

Can StarCorp survive this? Can I quote you as saying "No Comment?""

David finally gets rid of Tim. All breathe an audible sigh of relief.

Rocky "Tim's got some good points – should we be expecting more legal trouble?"

Legal:
Anna summarizes the legal position that StarCorp faces.

Anna "It doesn't do us any good to start speculating now, but:

- Nebular is seeking damages from us if their customers bring actions against them.
- Some of our own customers are threatening to sue us for down time; apparently some of them still believe we didn't get the system back up in time.
- We've also had a number of threats to sue for breach of privacy – Boylan is talking about a class action.
- Some other clients are concerned that their confidential business information may have been breached."

♦ ♦ ♦

Rocky "When I spoke to Brenda she said she wants a full internal investigation into what happened. She's very unhappy – someone could get fired for this."

Kelly "Well, at least it won't be my job on the line – you lot never listen to me about following security policy."

Process:
Yet again, the managers in StarCorp demonstrate that teamwork is not one of their strengths.

How would you fix this problem?

Lucinda "I wouldn't be too sure – your security policies are not followed because they're just not workable. Look at the IRP – there's no way we could implement that in a reasonable time …"

Kelly "The timeframe isn't my fault; you were the one who negotiated the contracts with an eight-hour drop dead clause."

Lucinda "Kelly, those are standard service level contract terms – eight hours down time is pretty generous, commercially speaking. We couldn't get away with any more than that – our competitors would put us out of business."

Process:
Isn't it fortunate that Rocky's "operations manager" leadership is keeping this team focused on the real issues, despite their lack of teamwork.

Rocky Step in to calm things down – suggest that Anna considers the strengths and weaknesses of Nebular Networks' case and they all reconvene later in Anna's office.

♦ ♦ ♦

Lights down; Scene ends.

Act 2, Scene 2

Lights up; the team is convened in Anna's office.

♦ ♦ ♦

Anna "Welcome everyone. I have had a chance to go through the particulars of Nebular Networks' claim. They make a couple of specific allegations:

Legal:
A list of all the things that StarCorp faces from their aggrieved customer Nebular Networks.

These are real allegations that could be levelled in a scenario like this.

- Our system was not secure in the first place.
- Our security policies were deficient.
- Our procedures for screening and supervising employees were inadequate.
- Even if our procedures and systems were adequate, we failed to follow our procedures and operate the system properly.
- Specifically, we failed to follow our IRP (which they claim was unworkable)."

Kelly "The IRP wasn't unworkable; we decided to ignore it on purpose because Lucinda didn't want to follow it … against my advice."

Legal:
An important point – when litigation starts, things get ugly.

David "Do they accept we did anything right?"

Anna "This is litigation: things get ugly … What we need to do now is work on our defense."

♦ ♦ ♦

Rocky "Let's start at the beginning. Can we show that we had a secure system? How do we do that?"

Anna "We have to show that our security was commercially reasonable, and that it was appropriate for the particular business application.

Legal:
A legal view on what constitutes commercially reasonable security.

We could do that by showing conformance with recognized standards or generally accepted industry practices.

If this goes to trial, we would have to get some independent expert evidence to support us.

We'll also need to show that the system was operating properly. Was there anything unusual on our last audit?"

Technical/Process:
The crucial role of audits, to show some degree of due dilligence and good practice.

Rocky "Kelly, where is the last Audit Report?"

Kelly "We can't seem to find the last Audit Report."

Rocky "What do you mean? We need to find that PDQ."

Kelly "I can't explain it – no-one seems to know what's happened to it."

Process:
And don't forget that good practice includes maintaining secure records, especially of Audit Reports and associated response measures.

Anna "Rocky's right. We need to find it – we need it as evidence of our system security, and if we can't produce it, Brendan will think we have something to hide. He's bound to ask for it to be disclosed."

♦ ♦ ♦

Rocky "What about our security policy? We put a lot of time and money into developing that."

Kelly "The policy is fine ..." *(emphasize the word "policy")*

Process:
Policies are ineffective if they are not enforced.

The best mode of enforcement is buy-in from all affected, demonstrated from the top down, and supported by training and practiced as an integrated part of the job.

Anna "But did we follow it?"

Rocky "Yes, of course we did."

Kelly "Oh, come on – when was the last time anyone actually read any of it. There's dust an inch thick on most of this stuff."

Rocky "That's an exaggeration …"

Kelly "No it isn't – security ought to be a serious management issue; it has to be enforced from the CEO down. Brenda is more concerned about quarterly numbers than she is about security – it all just gets left to me. It isn't enough just to pay lip service to our security policy whenever we have an audit – it should be in practice every single day."

Technical/Process:
A balance must be struck between commercial efficacy and security, but if security is part of operations then it ceases to be seen as an overhead or a burden.

It's the company culture that controls this balance.

Anna "Are you telling me it's not followed?"

Kelly "Yes, I am saying that! It's commercial efficacy over security – whenever there's a conflict, we know which one has to give way."

Process:
Here we go again …

Lucinda “That’s because your policies are unworkable – how are we supposed to run a business if we have to spend all our time trying to make your half-baked security systems work …”

Another argument … Kelly accuses Lucinda of totally ignoring security issues; Lucinda insists Kelly’s policies are unworkable in a commercial (as opposed to a military) context.

Kelly “Look, the security policy review is overdue, and I can’t even get it started because no-one is interested.”

♦ ♦ ♦

Rocky “OK, let’s move on.”

Anna “What do we know about Johnny?”

Rocky “Not much to say really – he’s a bright guy, good background. Everything checks out OK.”

David “Wasn’t there a big fuss a while back about some guy getting promotion ahead of him? Something like that …”

Process:
Now we get to investigating reasons why Johnny – an insider with wide permissions in the IT system – might have made this attack.

Rocky “Oh, yes … but he got over that. He wasn’t right for the job anyway – wrong temperament.”

David “He was pretty sore at the time. Maybe this was his idea of payback!”

Anna “Maybe. We shouldn’t be surprised; a lot of attacks come from employees with grievances. Did anyone look into this during his last security review?”

Rocky “Probably. But Johnny’s been doing this job for years; no-one could have imagined he’d do anything like this.”

Anna “How was he in a position to break into Nebular’s system? What about access controls?”

Kelly “That’s just not an issue. Johnny *had* all the necessary access rights and clearances. He needed them to do his job.”

Anna “How closely was he supervised?”

Kelly "He was supervised, but no-one knew this job better than Johnny … he probably didn't need much in the way of supervision."

Legal:
Legal assessment is that the company did not perform well in managing Johnny, considering it placed him in a good position to mount this whole intrusion attack – including on a customer's data – alone and with no supervision.

This will not look good for the company if the case comes to trial.

Anna "That's not good. It looks as though Johnny was able to build up his own little domain, and nobody would have had the faintest idea what he was doing.

Added to that, it seems that no-one realized he was harboring a grudge.

What about his financial and home situation? Was he getting divorced, under financial pressure?"

Rocky "We'll need to look into that, Anna."

Anna "Yes we will, because it's up to StarCorp to make sure our people are properly screened, *and* to make sure that if someone turns out to be dishonest, that they cannot do any harm."

♦ ♦ ♦

Rocky "None of this sounds very good, but how much trouble can we really be in here? There's nothing unusual about our set-up. I don't think we're any worse than anyone else in this business."

Anna "No, but no-one's set-up looks perfect when you put it under a microscope. It's a question of what will look reasonable to a jury.

Our procedures will be measured against normal industry practices, so if they look good by that standard we may be OK, but it isn't a foolproof test. Just because everyone you know operates in a similar way to the way you do, doesn't mean that a court will find it satisfactory."

Legal:
Common practice is a partial defense, but should not be taken as a foolproof test. A company should also seek to use best reasonably available technology.

Rocky "That's not very reassuring. If the court doesn't like it, how much is it going to cost us?"

Anna "That depends on what losses Nebular Networks can prove.

Their claim is huge, but part of it arises from an assumption that they would have won the government contract if Johnny hadn't sold information about their bid to a competitor.

That's a complex issue – we'll have to wait and see what they come up with."

Rocky "What about insurance? If we lose in court, can we get our money back?"

Anna "We have insurance, but I'm going to have to check the details of the policy.

You already know that insurance doesn't cover everything.

I know we're covered for dishonest employee acts related to our own systems.

We are also covered for civil liability to third parties: negligent acts, breach of statutory regulations, and also for breach of trust.

The policy assumes our security system was adequate – we'll have to show that it comes up to industry standards.

If we make a claim, the insurers will send in a loss adjuster to investigate.

There's also a cap on claims, so even if we have a valid claim we may not be able to recover the entire loss."

Legal/Process:
Insurance helps but is not the full answer.

There isn't much history for big damages claims arising from losses due to breaches of IT security.

What is certain, however, is that IT security breaches cost businesses millions worldwide, and it's only a matter of time before a financial loss becomes so great that it comes to court.

The Open Group Active Loss Prevention Initiative (ALPI) helps here – it includes lawyers, insurers, and finance institutions.

Rocky "Are you saying we might not be covered?"

Anna "There isn't much history for claims like this; it's hard to predict."

♦ ♦ ♦

David "You're really a ray of sunshine today, aren't you Anna? What do you suggest we do?"

Anna "I'll draft a defense; we'd better have another meeting to look at our evidence. Let's take a break for now."

Rocky "OK, but please work with David – he'll need to put together our public message."

♦ ♦ ♦

Lights down; Scene ends.

Act 2, Scene 3

Lights up; the team is assembled around the table in Anna's office.

♦ ♦ ♦

Anna "Good morning. We're here to discuss the state of evidence. Kelly, can you tell us what was and was not captured in the abbreviated system backup process?"

Kelly "Before we halted the normal backup procedure, we backed up Johnny's machine. We also backed up about half of the other workstations. In terms of servers, we finished one of the two replicas of the order-processing application server, and the machine at our end of the Nebular Networks link."

Legal:
More evaluation of the defense evidence, from the legal perspective.

Anna "It sounds like all the most relevant machines were backed up. That's good.

It's also good that the backups have been in escrow since the search and seizure order – so we can't be accused of tampering with them.

The downside is that Nebular has all the material information, including the logs showing that it was our system that attacked them, the files showing that their materials were on Johnny's hard drive, and the backup log showing that we didn't follow our procedures to the letter.

We're still arguing about what will and won't be disclosed; we have a hearing with Judge Landis tomorrow. He will make decisions, but anything which is relevant to the case is likely to be disclosed; the good, the bad, and the ugly."

♦ ♦ ♦

Kelly "Anna, when we were going through the backups, we found something interesting in the Nebular Networks' material on Johnny's machine. It's related to the government bid."

Anna "Interesting how?"

Technical/Legal:
Kelly's investigative dilligence on the customer's damages claim reveals evidence that will help to refute it.

It is important when incidents are discovered to continue with sound investigation to reveal relevant evidence.

Kelly "Interesting in the sense that they're claiming we cost them a chance to win the bid – apparently not everyone at Nebular thought they *had* a chance."

Anna "Could you send me a copy of that information, Kelly? Please send me a paper copy only, and don't give it to anyone else; even though it's in our backup, it's still Nebular Networks' proprietary information."

♦ ♦ ♦

David Express again very grave concerns about disclosure. Ask whether there's any way to prevent this information from becoming public – Tim is living up to his name "the Terrier" sticking his nose in everywhere … Ask whether there is any kind of court order we can get to stop Nebular Networks making the information public.

Anna "We probably won't be able to prevent evidence introduced in a trial from becoming public. The court will allow Nebular Networks to use whatever it needs to support its case."

Legal:
When litigation starts, all relevant company information (from defendant and claimant) can be demanded and must be revealed – albeit under non-disclosure – to the court.

David Ask whether the material the Judge will force StarCorp to disclose can be restricted; the order itself will of course be public. For example, Nebular Networks is asking for information about security going back years … security policies, reviews, audit reports, etc. (*Wave a bunch of court papers at Anna.*) "Surely, they're not entitled to know every detail about how we operate?"

Anna Explain that the court will not permit a "fishing expedition" by Nebular Networks, but that orders for disclosure are likely to be extensive.

♦ ♦ ♦

Kelly "A disclosure order will probably catch that Audit Report we had a few problems with last year, then, won't it?"

Anna "What was wrong?"

Kelly "Nothing really bad; we had made some errors setting up our access control policy, configuring our firewalls, that sort of thing. All the problems were the sorts of things you find in any IT shop, but that doesn't mean they'll look good in the newspaper."

Technical/Legal:
Audits of processes are "good"; they are intended to prove the effectiveness and practicality of the process, and to reveal any shortcomings.

An Audit Report is only damaging if identified shortcomings are not remedied and re-checked as effective.

Anna "They're probably going to get disclosure of that – it's not too far back in time and it supports their case about the inadequacy of our security."

Kelly "But we acted perfectly responsibly; we took corrective actions just as our processes specify, and put everything right immediately. At the end of the day we got a clean bill of health. They shouldn't be able to use the report against us if the jury knows anything about audits!"

Anna "You're right; if we followed our procedures correctly and implemented corrective actions which led to us passing the audit, that will be a point in our favor. But Nebular Networks will try to use any variances as evidence that we didn't have commercially reasonable protection. And the jury won't know much about audits – that's the problem with jury trials."

♦ ♦ ♦

Rocky Point out that if we have to produce everything they ask for, it will cost a fortune. Ask who will pay for all this.

Legal:
Who pays for providing all the evidence?

Anna "It depends on who wins the case. If we win, we may be able to recover the costs of defending ourselves."

♦ ♦ ♦

Rocky "Don't we get to ask them to disclose anything?"

Anna "Yes, we will be asking them for a lot of damages."

♦ ♦ ♦

Lucinda Ask what the system backup shows from an evidential perspective.

Anna "There's enough to show Johnny's activities and that he's the source of the attack on Nebular Networks …

The fact that we didn't manage to complete the backup won't impress the court. Brendan will claim that it is evidence of our inadequate security procedures."

Process:
This is where the consequences of not completing the IRP begin to come out.

Kelly "Cutting the backup short certainly seems like a great idea now doesn't it, Lucinda? I told you this would get us into trouble."

Lucinda "Kelly, it was your half-baked security which got us into this mess, and your half-baked IRP which failed to get us out."

(Argument ensues.)

Process:
Kelly and Lucinda have another spat about the IRP.

Rocky "Let's move on."

♦ ♦ ♦

Anna "There's one more thing. The scope of Nebular Networks' discovery order also covers your letter of protest, Kelly."

Kelly "Which one? I've written Brenda dozens of letters complaining about the lack of co-operation I get."

Anna "I'm talking about the letter you wrote objecting to the abbreviated backup procedure."

Rocky "How did they find out about that?"

Anna "I am not sure that they do know about it, specifically – but it clearly falls within the scope of one of their requests, so we are going to have to disclose it."

Lucinda (*half jokingly*) "Can't we just lose it?"

Legal:
In litigation, absolutely ***all*** *relevant information has to be revealed to the court – nothing can legally be excluded, though it may be afforded special protection over non-disclosure in court.*

Anna (*firmly*) "Not unless we want criminal charges against us as well as civil ones. We might be able to claim privilege because I was copied on the letter, but it's a weak argument and we shouldn't count on being able to prevent disclosure."

David "Smart move putting our weaknesses in writing, wasn't it, Kelly?"

Kelly "I don't see how the letter could make a difference; any idiot can see that we didn't follow our procedures."

♦ ♦ ♦

Rocky "Talking about losing things, have you found the missing Audit Report yet?"

Process:
Another reminder of the importance of maintaining secure records, especially of Audit Reports and associated remedial measures.

Kelly "No, I can't understand it – it's just vanished; we have all the Audit Reports except that one."

Anna "We really need to find the missing report, and *soon*."

David "Could Johnny have stolen it to cover his tracks?"

Kelly "I'm looking into it, but there's no evidence of that yet."

♦ ♦ ♦

Rocky "There are just too many problems here – and if they become public, StarCorp is in serious trouble even if we win the case – can't we negotiate a settlement?"

Legal:
The discussion begins on whether or not to settle out-of-court, bringing out the key issues that any company in StarCorp's position has to evaluate.

David "I agree, we ought to try and settle: we just can't risk the publicity."

Kelly "Absolutely not; we can't let Johnny off-the-hook, and we can't just let Nebular Networks blackmail us!"

Rocky "David is right, we can't risk the publicity – we've got to settle this before we're ordered to make any more disclosures. I've spoken to Brenda; that's her preferred option too."

(to Anna) "Do you think you can negotiate a settlement? And if they agree to settle, can we stop them making any of this public?"

Kelly "I can't believe we are just going to pay hush money to these pirates!"

Anna "I can try negotiating a settlement. I can make confidentiality a condition of any settlement.

I can't restrict matters that are already in the public domain, like the stuff that Tim has already put in his newspaper.

Settling the matter will mean that we don't have to make any further disclosure, so that should help."

Rocky "I think you should do that."

♦ ♦ ♦

Legal:
If you involve your insurers, they too will bring in professional loss adjusters to conduct their own investigation on the actual losses sustained. Their findings will be outside the company's control so may also leak out …

Lucinda "If we have to settle, can we make an insurance claim and get some of our money back?"

Anna "If we do, then the loss adjusters will come in to do an investigation."

Rocky "I suppose we can't be sure that *that* won't leak out."

David "Especially not with Tim and his … **** ... newspaper around!"

Rocky "Let's see what it will cost to settle – if we can absorb that cost, then maybe we won't need to make a claim."

Anna "OK, I'll set up a meeting with Brendan."

♦ ♦ ♦

Lights down; Scene ends.

Act 2, Scene 4

Lights up; Kelly is sitting in a chair; Anna and Brendan are standing in front of him.

♦ ♦ ♦

Legal:
This is an example of how a legal deposition led by the claimant's lawyer preceding a trial might go.

Read on, and think about how a proud professional defense witness – perhaps you – might react under the questioning of the claimant's lawyer.

Brendan "I'm Brendan Boylan. This is a deposition in preparation for the civil action that Nebular Networks is bringing against StarCorp. In a minute I'm going to ask you some questions, but first, could you please state your name and position."

Kelly "Col. Kelly A. Rider, US Army Retired. I am the IT Security Manager for StarCorp."

Brendan Mr. Rider, your company has designated you as the person most knowledgeable about the breach in security that your company experienced, how it has spread out to effect others, and the security procedures your company uses."

Kelly “I’m retired, but I’m still entitled to be referred to as “Colonel Rider”, if you please.”

Brendan “Are you the most knowledgeable person about each of these issues?”

Kelly “Yes.”

Brendan “Is there any one in the company that we should be talking to instead of you, who knows more than you do about what happened and why?”

Kelly “No, of course not. Nobody else really understands much about security.”

Legal:
The lawyer first establishes who is the defendant’s senior expert responsible for security.

Brendan “Your fellow managers understand selling products and shipping orders, but not network security, right?”

Kelly “Security is my job, but they have to know something about it. I mean, they use the system. I don’t mean that they, the system users, are clueless about security and network issues.”

♦ ♦ ♦

Brendan “Well, let’s find out just how clueless StarCorp really has been. Somebody hacked into your network this week, correct?”

Kelly “What do you mean by “hacked”?”

Brendan “Why don’t you tell me what you mean by “hacked” and we’ll use that definition.”

Kelly “I don’t use the word. But I think people mean that someone gains access to the network who is not supposed to have access, or uses access to cause damage to the network or the people and systems that use it.”

Brendan “Fine. Did that happen this week?”

Kelly “Yes.”

Brendan “Does StarCorp know who did this?”

Kelly “Yes.”

Legal:
The lawyer then establishes what the defendant's employee did when mounting the attack and how their organizational structure allowed it to be possible.

Brendan “Who?”

Kelly “Johnny.”

Brendan “We'll get back to who that is. But tell me what he did.”

Kelly “He appears to have accessed a Nebular Networks computer.”

Brendan “He did this from within your offices? What access codes, passwords, or permissions did he need to pull this off?”

Kelly “His job required him to have the highest-level access.”

Brendan “Who else in the company has that level of access?”

Kelly “Just me.”

Brendan “You are a relatively high-level employee and young John is not, correct?”

Kelly “That's right.”

♦ ♦ ♦

Brendan “The intrusion had an effect on your own functions, your own order-processing, and on Nebular Networks, correct?”

Kelly “Yes.”

Brendan “What happened to your order-processing?”

Kelly “It shut down.”

Brendan “For how long?”

Kelly “Seven or eight hours. Definitely less than eight hours.”

Brendan “How long did it take you to identify the source of the intrusion?”

Kelly “As I said, a few hours. It took a few hours.”

Brendan “What did you do to preserve the record of what had happened in your system and how it had interfered with your customers and partners?”

Kelly “Well, we backed up the system.”

Brendan “How long did that take?”

Kelly “Seven or eight hours.”

Brendan “And normal operations were down that entire time?”

Kelly “Yes.”

Brendan “That is a very short backup isn’t it?”

Kelly “We worked very fast.”

Brendan “Did you back up all the activity in the system to allow us to recreate what happened and how?”

Kelly “We backed up all the relevant servers and Johnny’s machine.”

Brendan “Let’s try this Mr. Rider: did you back up all the central file servers?”

Kelly “It’s Colonel Rider. We backed up at least one copy of each replicated server cluster. The replicas in each cluster are all the same.”

Legal:
The lawyer then establishes that the defendant’s IRP to preserve all evidence was not completed, and why (they had to restore system operation before completing backups).

Brendan “Did you back up all the workstations?”

Kelly “No.”

Brendan “Why not?”

Kelly “There wasn’t time.”

Brendan “Why not? What was the hurry?”

Kelly “We couldn’t have the system down that long.”

♦ ♦ ♦

Brendan “You have an Incident Response Plan, don’t you?”

Kelly “Of course we do. I wrote it.”

Brendan “Great. So it is a complete and careful plan to respond to a security breach.”

Kelly “Absolutely.”

Brendan “Does your IRP require a complete back up of the entire system?”

Kelly *Silence*.

Brendan “Mr. Rider, your plan requires a complete backup, does it not, of every server and workstation in the network?”

Kelly “Colonel Rider. And yes, it does.”

Brendan “But you did not do that.”

Kelly “No.”

Legal:
He next extracts an admission from the defendant’s expert witness that the incompleted IRP process could have resulted in lost evidence.

Brendan “So you cannot tell us today if data relevant to this break in – data that would show how it happened, the damage it caused, the damage it caused to my client – if that data is now gone. You can’t tell us that.”

Kelly *Long pause*. “We don’t believe anything important is missing.”

Brendan “So you decide what’s important?”

Kelly S*ilence.*

Brendan “The answer, Mr. Rider, is that you don’t know what hasn’t been backed up because it hasn’t been backed up.”

Kelly “We did not back up every workstation in the system, no. It wasn’t practical.”

♦ ♦ ♦

Brendan “In fact, your management’s failure to back up the entire system amounts to a rejection of your IRP, doesn’t it?”

Kelly “That’s pretty strong. I am not sure I would say that. The backup was not complete, but all the systems involved in the attack were backed up.”

Legal:
And then extracts a further admission that the defendant (StarCorp) decided to abort their own IRP because it was unworkable – i.e., not fit-for-purpose because it could not be completed within their contractual eight-hour limit.

Brendan "But you did say exactly that, Mr. Rider. The court reporter has marked this letter as Exhibit 1 for the deposition. Please read it and tell me what it is."

Kelly "I wrote this letter. It was a private letter. I expected it to remain private."

Brendan "That is obvious. This is litigation, Mr. Rider. Nothing is private. If it was written down, we will read it. If it was said, we will hear it. As you say in your letter, StarCorp management dismissed your IRP the first time it was needed, correct."

Kelly "Yes. And it's Colonel Rider."

Brendan "And they felt that the plan was unworkable? Colonel Rider?"

Kelly "In the heat of the moment, but yes."

Legal:
As Anna said earlier, the claimant's lawyer also says: "In litigation, nothing is private. If it was written down, we will read it. If it was said, we will hear it."

Brendan "In any event, they resisted the procedures that their own security department deemed necessary, correct?"

Kelly "Yes."

♦ ♦ ♦

Brendan "Now that we know you did not follow your IRP, let's find out about your Security Plan generally. You have one of those, right?"

Kelly "Of course we do."

Legal:
Next, the defendant's Security Plan comes under scrutiny.

Do you have a Security Plan as well as an IRP/disaster recovery plan?

Brendan "Who prepared it?"

Kelly "I led the effort to create that plan."

Brendan "Has the plan been updated in the years since it was written?"

Kelly "Yes. Several times."

Brendan "Have you suggested improvements from time to time?"

Kelly "Sure. That's normal. You can always make a plan better."

Brendan "Have your recommendations always been adopted?"

Kelly "Not always."

Brendan "Why not?"

Kelly "Security is expensive, both in time and money. And managers have different priorities."

Legal:
Customers and courts place high value on the security their suppliers provide; revealing a bad approach/record on this could lose a supplier a lot of business.

Brendan "Are you saying that StarCorp management places time and money ahead of the security of its customers and partners?"

Anna "I object, Mr. Boylan – do you want to let Colonel Rider answer, or do you already have your own answers prepared for the court?"

Kelly "I did not say that."

Brendan "Do you consider your Security Plan to be state-of-the-art – the best protection possible, Major Rider?"

Kelly "The rank is Colonel, Brendan. Not Major. And I think that it is a very good plan."

Brendan "Good enough to stop the kinds of intrusions that we can expect in this business?"

Kelly "Definitely. I have been in this business for many years. I know how to secure a network."

Brendan "But it did not stop this intrusion, nor did it protect Nebular Networks, did it?"

Kelly "No. In this case it did not."

Legal:
Criminal attack does not absolve a company from its share of responsibility if its IT systems are used in an attack.

Brendan "If it is such a good plan Mr. Rider, why didn't it work?"

Kelly "It's Colonel Rider, son. There was a criminal attack. You can't predict criminal behavior."

Brendan "Isn't a Security Plan designed to predict and block criminal behavior?"

Kelly "I don't think any plan could have blocked what happened here. A trusted employee, who had to have high-level access, turned against the company."

♦ ♦ ♦

Brendan “We’ll ask about your trust in this employee in a moment, but let’s talk about your trust in your plan just now. Your Security Plan requires that you do a security audit from time to time.”

Kelly “That is correct.”

Brendan “When was the last time that it was audited?”

Kelly “A few months ago.”

Brendan “What were the findings of the last audit?”

Legal/Technical:
This emphasizes that security audits are “a good thing”, and very helpful in a defense case.

Kelly “I don’t know them all off the top of my head.”

Brendan “Did the security system pass or fail the audit?”

Kelly “It is not as simple as pass or fail. The point of an audit is to identify and correct system weaknesses.”

Brendan “The Security Plan requires the audit findings to be compiled in a report.”

Kelly “That’s right.”

Brendan “You were required to produce that report at this deposition. Have you brought it with you?”

Kelly “Uh, no.”

Brendan “Why not, Mr. Rider?”

Kelly “Colonel Rider, son. We have not been able to locate the last Audit Report. We’re still looking for it and we will turn it over as soon as we find it.”

Legal:
However, you have to preserve your records of the audit and your remedial actions arising, so as to be able to produce the evidence of your due dilligence.

Brendan “You take audits seriously, don’t you?”

Kelly “Oh yes.”

Brendan “But you don’t have the record of the audit. You can’t even prove that there was an audit, can you?”

Kelly “There was an audit; we just can’t lay hands on the report just at the moment.”

Brendan "Or you are in the process of writing a fictional report right now, to find later?"

Kelly "I will not put up with that kind of offensive insinuation, you little snot."

Brendan "Which do you think will offend the jury more? Losing the report by accident or losing it on purpose?"

Anna "Mr. Boylan, if you have any more questions to ask, why don't you do so. Neither Colonel Rider nor I need to put up with gratuitous abuse. Kelly, you don't need to respond to anything which isn't a question."

Brendan "These are precisely the questions that I am going to ask Mr. Rider in front of the jury. He can answer them at that time if you're both more comfortable that way. Let's see where we are Mr. Rider. You are the lead manager responsible for network security, correct?"

Kelly "It's obvious you've never been anywhere near an honorable institution like the military, but get the rank right. It's *Colonel* Rider. I have a lot of jobs at StarCorp. Security is one of them."

Brendan "How about this: you are designated by StarCorp as the person most knowledgeable on all network security issues."

Kelly "Yes."

*Legal:
Here is the claimant lawyer's assessment of the defendant's legal position as so far revealed in this deposition.*

Brendan "And you have told us that you know more on this subject than anyone else. And you can't give us the complete picture of what happened in this attack, because you did not do the required backup, you can't tell us if your system even passed its security audit, or if there was an audit, and you did not know that your own assistant Johnny – with the highest-level access in the company – was seriously angry at StarCorp and bent on causing havoc?"

Kelly "We could not know that Johnny was planning an attack."

♦ ♦ ♦

Brendan “Let’s talk about what you knew about Johnny. Johnny has worked for StarCorp for quite a few years?”

Kelly “Yes. He was here when I arrived.”

Brendan “He works for you, correct?”

Kelly “Yes.”

Brendan “Did you do security reviews of Johnny?”

Kelly “I didn’t. He was hired before I got here.”

Brendan “Did anyone do a security review or a background check?”

Kelly “I am sure that someone did when he was hired.”

Brendan “Is that in a file somewhere, or is it hiding with the mysterious Audit Report?”

Anna “Objection. Drop it, Mr. Boylan.”

Kelly “I haven’t looked for it, so I don’t know where it is.”

Brendan “Was he screened regularly, yearly?”

Kelly “Yes, we do annual performance reviews. I did Johnny’s.”

Brendan “But you did not do a regular security review of this employee.”

Kelly “No. They are not required.”

Brendan “What kind of performance reviews did he get? Keep in mind that I can get Johnny’s file.”

Kelly “Pretty good. He was good at his job.”

Brendan “But he had been in the same position for several years, and not promoted, right?”

Kelly “That’s true.”

Brendan “If he was so good at his job, why wasn’t he promoted?”

Kelly “Other people were better suited for the jobs.”

Brendan "So he was passed over."

Kelly "You could put it that way."

Brendan "I just did. And he was angry about not being promoted?"

Kelly "I don't know that he was angry."

Brendan "Well, Mr. Rider, we all know now that he was angry about something. The question I have for you, as his supervisor, is did you know he was angry?"

Kelly "No."

Brendan "But the company trusted him."

Kelly "Yes."

Brendan "Thank you very much; I have no more questions."

Legal/Process:
The defendant StarCorp has not shown due dilligence in regularly doing a security review on its key IT security employee (Johnny), yet continued to give him full access to crucial defendant ***and*** *customer IT systems and data.*

♦♦♦

Anna "Mr. Boylan, I have just a few questions for Colonel Rider on behalf of StarCorp."

Brendan "Go ahead."

Anna "Have you reviewed the data that was taken by Johnny from the network?"

Kelly "Some of it. Not all of it."

Anna "Have you reviewed the files that he downloaded from Nebular Networks?"

Kelly "I have reviewed many of them, but there are quite a few that I have yet to go through."

Anna "You reviewed those files as part of the disaster response effort?"

Kelly "Yes. I had to determine what the files contained – viruses, trojan horses, that sort of thing."

Anna "Did those files include any of Nebular Networks' own internal memoranda concerning its bid for various government contractors, and the strength of that bid?"

Brendan "Objection. Hold on here. None of that is relevant to StarCorp's liability for the break-in to our system. You are just showing that StarCorp breached our confidential data."

Legal:
Here is an important formal declaration from the defendant that the claimant is overstating the extent and value of their claim for damages.

Anna "Relevant to liability or not, Mr. Boylan, I am getting to the issue that you have argued to the court: that StarCorp has prevented Nebular Networks from obtaining a valuable contract. The files that Colonel Rider reviewed paint a very different picture."

Brendan "Nonsense. But this isn't a conversation we need to have on the record. We don't need to take up any more of Colonel Rider's valuable time."

♦ ♦ ♦

Lights down; Scene ends.

Act 2, Scene 5

Lights up; Brendan, Anna, and the team are sitting at a conference table in the StarCorp offices.

♦ ♦ ♦

Anna "Mr. Boylan, in view of the documents you've turned over in response to our discovery motion, and in view of the memo you'll have to introduce if you want to demonstrate that the intrusion came from our systems, it's very clear that Nebular Networks has not sustained any damages."

Legal:
The defendant and claimant lawyers discuss the relative strengths of their respective cases ...

Brendan "Anna, that's speculation and you know it. Your employer's incompetence has cost us an important bid, and we're entitled to recover our losses."

Anna "I'm afraid it's your government services division's incompetence which cost you the bid, and I'm also afraid your own documents prove it. We acknowledge that your client spent some time and money recovering IT systems from the incident, and StarCorp is prepared to reimburse overtime and actual expenses for that effort."

Brendan "We can see how the jury looks at it. I can't imagine StarCorp's shareholders will be eager to have your miserable security on display in court, though."

Anna "Fine, Brendan; have it your way. You should be aware that we'll be filing a claim to recover the costs of this frivolous action from Nebular Networks if you proceed. I'll see you in court."

Long pause while Brendan and Anna try to stare each other down.

Legal:
... and effectively agree to explore whether their respective clients will entertain an out-of-court settlement.

Brendan "Listen, Anna. I'll talk to my clients if you like, but I really don't think they'll go for any of this; StarCorp's responsibility is just too clear. Give me a minute to call and I'll let you know."

Brendan exits.

♦ ♦ ♦

Rocky "Well, what do you think?"

Anna "I'm not very optimistic. Brendan's good, and the way he grilled Kelly in the deposition makes it clear he's going to drag us through the mud to get us to go for a big settlement."

David "I don't understand. The courts should throw things like this out!"

Legal/Process:
Lots of organizations suffer losses they don't report – they keep quiet because they're worried about their reputations. StarCorp's bad luck is that another company knows what happened and can use the threat to StarCorp's reputation to go to law with a claim.

Anna "You probably understand better than anyone else, David. Lots of organizations suffer losses they don't report – they keep quiet because they're worried about their reputations. Our bad luck is that another company knows what happened and can use the threat to our reputation to improve their bottom line.

The law doesn't give us any shield if we report our losses – in fact it punishes us with liability. And in general our insurance policies exclude security-related losses. It's a bad situation."

Legal:
The law doesn't give companies any shield if they report their losses due to an IT system attack – in fact, it punishes them with liability. And, in general, company insurance policies exclude security-related losses.

Lucinda "Surely somebody must be working on this problem? Don't we belong to trade associations, or lobbying groups? Does the security community have someone we can talk to?"

Kelly "We could talk to our ISAC, or InfraGuard."

Rocky "I thought ISACs were just for the financial industry?"

Kelly “No, various industries are setting up ISACs, but even if there’s one we can join, we won’t get much help with all these liability and insurance issues.”

Process/Legal/Technical: The Open Group Active Loss Prevention Initiative is bringing lawyers, insurers, auditors, and technologists together to talk about all the issues in IT security in a holistic way.

Anna “You know, there might be a place to go. I’ve just read a story about something called the Active Loss Prevention Initiative which is bringing lawyers, insurers, auditors, and technologists together to talk about all the issues in security in a holistic way.”

Rocky “That sounds promising – I’ll talk to Brenda about sending someone to meet with them.”

♦ ♦ ♦

Enter Brendan.

Brendan “Anna, can we talk?”

Anna “Certainly.”

They walk across the stage away from the team.

Anna “Do you have an answer for me?”

Brendan “Anna, your employer’s position is very weak.”

Anna “Just give me the answer, Brendan.”

Brendan “Against my advice, my clients are open to a settlement.”

Legal:
An out-of-court settlement is reached.

Most parties much prefer to do this to avoid huge litigation costs and damaging revelations.

Anna “Actual costs incurred responding to the incident, with strict confidentiality of all details of the incident, and no admission of wrongdoing?”

Brendan “Plus my fees.”

Anna “That’s ridiculous.”

Brendan “You want the settlement?”

Anna “Fine. I’ll prepare the paperwork.”

Exit Brendan.

♦ ♦ ♦

Anna *Walk back to the team*. "Nebular has agreed to settle on terms we can accept."

Cheers, collapsing in chairs, relief, celebration. The phone rings. It's Brenda. Rocky answers.

David "Anna, you're great! I was sure we were going to get killed on this one."

Process:
So that's where that embarrassingly missing Audit Report went!

Kelly needs to keep his own copy in a safe place where it can't be removed.

Lucinda "David's right, Anna. If you hadn't pulled off a settlement, we'd be in a lot of trouble."

Rocky "Brenda, they've agreed to settle."

Brenda "That's excellent news, Rocky. Especially given what I've just been reading in our last Audit Report."

Rocky "You have the Audit Report? We've been looking everywhere for it!"

Process:
The CEO recognizes significant organizational problems that need to be properly addressed.

Brenda "Yes; I pulled it from the files as soon as I heard about the incident. Our security system needs serious work. I need a meeting with you and Kelly immediately. And we have a lot of other work too. We need to look at our contracts, our insurance, our training, HR practices – I'm going to have to explain a lot of things to the Board, and we're going to make this a top priority.

But we can worry about that tomorrow. I want the team to join me at Morton's for lunch right now, and then I want everyone to take the afternoon off. You've all done an outstanding job on this."

Process:
The CEO also recognizes that her managers have achieved a good result for the company.

Rocky "Thanks, Brenda. I'll tell them right away." *Hangs up*. "That was Brenda. She is demanding to see all of us immediately to discuss this."

David "Is she going to grill us as part of her inquiry?"

Process:
Will the CEO also uncover during that celebratory lunch how much her senior managers need lessons in teamwork?

Rocky "She's very clear that we have a lot of problems and she's interested in how we're going to address them."

Lucinda "Is she still talking about people losing their jobs? I'm not going to take the fall for Kelly's failures."

Rocky "If you and Kelly can't learn to get along, I think Brenda will have something to say to you both. She thinks teamwork is one of the most important things we've failed to get right. What she really wants to know is how we're going to fix our processes to make sure we don't have to make compromises under pressure next time."

Process:
Aha – Rocky believes the CEO has recognized that a teamwork problem exists.

David "So can we stop worrying about our jobs?"

Rocky "Yes. In fact, Brenda's very happy with the way things have gone so far, but she doesn't think we're out of the woods. She wouldn't be surprised if we hear more from Brendan Boylan very soon. We'll meet at Morton's steakhouse as soon as you can get there, and you can ask her what she thinks in person. And call home and tell your families that you're very sorry, but you'll be home early."

♦ ♦ ♦

Lights down, Scene ends.

House lights up; applause.

Introduce Ian Lloyd for a description of the work of the Active Loss Prevention Initiative.

Audience Q&A

Process:
Detailed information on the ALPI is available at www.opengroup.org/alp.

About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, committed to a vision of **Boundaryless Information Flow** achieved through global interoperability in a secure, reliable, and timely manner.

The Open Group's mission is to drive the creation of **Boundaryless Information Flow** by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

The interoperability that characterizes **Boundaryless Information Flow** results in gaining operational efficiencies and competitive advantages. Through access to integrated information, across the extended enterprise and beyond, employees, trading partners, and customers are enabled and empowered.