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

Copyright © 2003 The Open Group

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

Boundaryless Information Flow is a trademark and UNIX and The Open Group are registered trademarks of The Open Group in the United States and other countries. All other trademarks are the property of their respective owners.

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.: 1-931624-29-1

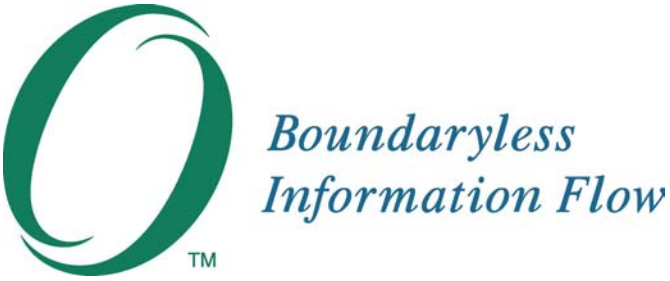
Document No.: W031A

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 complete annotated script is available in Doc. No. W031. 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 un-quantified 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.

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.