PICKING APART PCI

AN IANS EXECUTIVE ROUNDTABLE

New York City

SUMMARY OF FINDINGS

NOVEMBER, 2008

Featuring Materials From:

Tenable Executive Roundtable

A unique roundtable discussion on the most important issues facing IT leaders.

Tenable has partnered with IANS to develop and moderate a series of Executive Roundtables.

IANS is an independent research organization providing community-sourced decision support to IT professionals.

About Tenable Network Security

Tenable Network Security is the world leader in Unified Security Monitoring. They provide agentless solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis, and compromise detection.

Tenable is the sole sponsor of the Nessus vulnerability scanner which provides to the Internet community a free, powerful, up-to-date, and easy-to-use remote security scanner. Nessus is currently rated among the top products of its type throughout the security industry and is endorsed by professional information security organizations such as the SANS Institute. Tenable estimates the Nessus scanner is used by more than 75,000 organizations worldwide. www.tenablesecurity.com

About IANS

IANS is the premier membership organization for practicing information security professionals. IANS' mission is to provide key technical and business insights to help members solve their most pressing professional challenges. IANS achieves this mission through a broad offering of services provided to its members—insightful events, thought-provoking publications, best-practice research, and unique networking opportunities. Learn more at www.ianetsec.com.

Context

This Executive Roundtable had two sections. First, participants discussed the *Harvard Business Review* case titled "Boss, I Think Someone Stole Our Customer Data." Participants then switched gears, discussing some of the most significant information security issues they are facing, with particular attention to PCI.

Executive Roundtable – Part 1: Case Study Discussion

Briefing Summary

- In a potential data loss situation, discern between what is "known" and what isn't.
- Have the right people involved, including the CEO, and understand each person's motivations.
- Organizations must identify all potential risks faced when an incident occurs (legal, financial, reputational, etc.) and determine what is most important.
- Data leak incidents require coordinated responses in many areas: legal, forensic, law enforcement, financial, and, most important, communications.
- One of the most common causes of data leakage is through email and messaging. However, this type of vulnerability is often overlooked.
- Important lessons can be learned from this case study on the importance of preparation, CEO engagement, security involvement, incident response planning, and the role that technology can play.
- With sophisticated email and content encryption systems available today, no organization has an excuse for not adequately protecting its data.

Background

The *Harvard Business Review* case titled "Boss, I Think Someone Stole Our Customer Data." was published in the *Harvard Business Review* in September, 2007.

This hypothetical case study focused on a small/mid-sized B2C retailer that had a long, proud heritage and a strong brand. The company (which was not yet fully PCI compliant) was informed by a bank of a potential data leakage. It was certain that 1,500 customers were affected and likely more.

The company knew it had an IT vulnerability (an open firewall), but was not certain if a data leak had actually occurred and if it had, was not certain if the open firewall was the cause.

Participants were provided with pieces of information concerning a potential data leak (the type of imperfect information that executives often possess when forced to make difficult managerial decisions) and were forced to think through how this company should respond and what lessons can be gleaned.

After developing an initial set of conclusions, participants were provided with an endnote which revealed additional information about the cause of the data leak.

Discussion Summary

- **Start by figuring out what is known and what isn't.**

  Even though it was uncertain whether the organization in the case study experienced a data leak, participants agreed that the situation presented major risks and should be treated with great seriousness.

"Everybody sees risk differently based on the chair they sit in."

  Participants agreed that the best approach is to take inventory of "What do we know?" Focus on the facts and immediately gather all relevant information.

  At the same time, it is also essential to identify what isn't known. (An example might be, "What is our legal obligation?") To help identify what isn't known it may be appropriate to enlist experts.

- **Focus on the people involved; understand their perspectives.**

  Dealing with situations such as this usually comes down to the people involved—their perspectives, emotions, and motivations.

"A huge mistake this organization made was not having a Chief Security Officer, and not having any security expertise at the table."

  It is important to define "who needs to be involved." Because of the potential implications of a data breach, the CEO and other senior executives need to be at the table. They must understand the risks and be ready to make difficult business decisions. An obvious omission in the case study is that this company lacked any person with information security expertise.

  Once the right people are at the table, it is important to understand each person's perspective, pressures, emotions, interests, and motivations.

- **Determining the right plan of action requires identifying the real and perceived risks to the organization.**

  The company in the case study faced many potential risks. These included legal/liability risk, reputational risk, financial risk due to lost business, and risks with investors.

  Many of these risks are affected not just by the reality of the situation, but by perceptions. (Even if the company hadn't done anything wrong, there might be a perception of data leakage, which could hurt the company's reputation and financial results. Perception is reality.)

- **After weighing the risks, organizations need to develop action plans in several different areas.**

  Participants envision action along several fronts. These include:

"You need the right expertise in all areas—legal, technical, communications."

  - **Forensics**. It is essential to enlist a forensics expert to help understand exactly what has occurred.
  - **Law enforcement**. Several participants saw an important step as contacting and cooperating with law enforcement, such as the FBI and Secret Service. However, others saw this as potentially

premature based on what is currently known. They thought that bringing in law enforcement without more knowledge of this situation could cause an escalation that was not desired.

- **Legal/regulatory**. The company might have obligations to comply with disclosure requirements. It is necessary to have legal counsel with expertise in this area to provide sound and practical advice.
- **Communications**. These are perhaps the most important decisions to be made: whether to communicate to customers/employees, what to communicate, and how to communicate.

  It was agreed that a communications plan is needed and that experts should be enlisted to develop and execute it.

  However, it was not agreed what this plan should entail. Participants had differing perspectives.

  - *Proactive communication*. Some participants believed that the company should be proactive. It should contact customers, share what is known, and describe the specific actions the company is taking. Those advocating this strategy believe that being proactive enables the company to control the message and helps the company's reputation. They believe that consumers are no longer alarmed at such breaches and would prefer a company disclose, rather than sit on such information. (The Tylenol example was mentioned where J&J proactively pulled Tylenol from the shelves. This short-term revenue hit built trust with consumers and is seen as the ideal way to behave in a crisis.)

"I think you have to tell customers what you know as early as possible. You should be very careful in how you do it, but you would rather tell them earlier than later."

"But you don't really know anything yet. Why say anything if you don't know anything yet? It might cause more problems."

  - *Gather more information before disclosing*. Others felt it was premature to disclose until more was known. They thought that disclosing at this stage could be unnecessarily opening a Pandora's box. (Those in this camp argued that the Tylenol situation was different because more information was known when J&J acted than is known here.)

  Regardless of the timing and the communication tactics employed, it was agreed that when communication takes place the specific messaging is critical.

- **Many important lessons can be learned from this case study.**

  Among these lessons were:

"You need preapproved incident handling procedures."

  - **The need for advance planning**. The organization in the case study lacked a clear incident response plan; they were figuring things out on the fly. Participants agreed that organizations must have clear values and clear incident response plans.

    - *Values*. In a crisis, leaders will have to make difficult decisions based on imperfect information. Will the criteria for the decision be to minimize legal liability? To preserve the company's reputation? Companies that are grounded in a set of core values will find it easier to make these difficult decisions.

- *Incident response plans*. Every organization will have an incident at some point. Organizations should put together an incident response team, with representatives from all key functions, and should have clear incident response processes. Teams would be well served by engaging in drills and scenario-planning exercises.

"Yes, information is lacking and these decisions are hard, but these are the types of discussions that IT executives need to be prepared to have if we want a seat at the table."

- **The need for communications planning**. Communications decisions were the most critical decisions in this case study. Again, making such decisions on the fly doesn't yield the best results. Organizations need to have expert resources available and should contemplate, prepare for, and practice various scenarios.
- **The need for information security involvement**. This company lacked information and expertise about security. This illustrates the need for security to be at the table in the planning process and in the incident response process.

"Most CEOs don't really understand IT risks. We have to make them understand."

- **The need for early CEO engagement**. It is essential not just to involve the CEO after an incident has occurred, but to educate him or her now on the potential risks to the organization associated with data leakage. This requires quantifying the risks and showing examples of ill-prepared companies and the consequences of not being prepared (possibly by using tools such as this case study). The goal is to secure CEO support for efforts aimed at preventing data leakage along with processes for how to respond should it occur.

"People are the worst aspect of security, but they can also be the best aspect of it."

- **Technology can play a role**. While the case study was primarily about identifying risks, making difficult decisions, involving the right people, and preparing, this is a role for technology. The right technologies could have helped identify vulnerabilities and keep some data leaks from happening. It can help with forensics, can help with correlation, and can provide better network visibility—all of which are important to prevent incidents and/or respond to them.

Part 2: PCI Discussion Summary

After the case study, participants described steps they are taking to comply with PCI and to improve their overall security posture.

- **Complete PCI compliance may be a pipe dream.**

  Participants agreed that PCI compliance cannot totally eliminate data security risks. Organizations can be 100% compliant at one point in time and pass all of the scans and assessor tests. But networks are always changing. There are companies that continually pass the PCI assessments but are still hacked.

"You can never say you are 100% compliant."

- **PCI compliance is not the only answer.**

  PCI compliance receives mixed ratings. Among participant comments:

"The whole concept of PCI is a desperate attempt by the credit card companies to move some of the onus for data loss to merchants."

"PCI makes you do some common sense practices.… It pulls you up to a minimum standard."

Security concerns extend far beyond PCI compliance. Organizations are more concerned about data breaches, including the security of customer data and intellectual property. A participant from a tier one company summed it up. *"There's nothing wrong with being out of compliance; it's being out of compliance and having a breach that is the problem,"* commented a participant when asked how worried the company was about not being PCI compliant.

"Our business isn't covered by PCI or any other standard that dictates encryption, but we encrypt anyway. We look at PCI and other standards to learn things that we should be doing even though we aren't covered."

On the other hand, data breaches do not always result in customer losses. Participants pointed out that TJX and Hannaford do not seem to have lost customers, even though their data breaches were well profiled.

- **Data encryption is an important protection measurement.**

  Data encryption is a valuable security technique, even for those participants who are not PCI compliant. One company uses the .NET encryption routine for credit card data encryption; everything written to the database is encrypted; additional protection was added to manage encryption keys and prevent database administrator access.

"You have your policies and procedures but it really comes down to the people."

- **Liability involves both people and processes.**

  Liability associated with loss of sensitive data should not rest exclusively on the shoulders of security professionals; securing this data is the responsibility of the entire organization. Along with various technologies to secure data, data security requires that people in an organization are trained on security awareness and that processes are developed to keep sensitive data secure.

- **There are many aspects to managing risk.**

  Risk management must address the full scope of business issues. For instance, the effort to fully audit a large bank that handles credit cards may take two years. While credit card fraud may result in large financial losses, the actual costs may actually prove less than those involved in a full organization audit.

"There are companies 'in the nirvana' of having all the controls in place."

Usually, the Fortune 100 or 1000 companies don't need to worry about PCI because they have all the access controls in place, unlike smaller companies that lack the resources to do so. Those "in the nirvana" can demonstrate actual cost savings due to reduced loss and less headcount.

One concern was how to map practices to multiple sets of regulations. Archer Technologies was recommended as a vendor that can pull together multiple sets of information from various tools to help companies map security practices against regulation requirements.

"You need to look at other basic issues beyond those specifically addressed by PCI."

- **Standards are here to stay.**

  The ITIL® framework defines processes to facilitate PCI implementation. For instance, ITIL includes sections on creating a culture of change management and configuration management.

  Standards are expected to evolve over the next few years, say participants: PCI, HIPAA, and other standards will become stricter, ISO standards will assume greater importance.

- **Vulnerability management is critical.**

  A security program must proactively guard against a range of potential vulnerabilities such as poor asset management. For instance, large organizations do not always track the precise number and location of laptop PCs issued to employees. When obsolete laptops are replaced with new models, there is potential data security risk when the obsolete laptop is not returned and properly disposed of. For example, teenager family members have received old laptops containing proprietary customer data, network diagrams, and other confidential information.