Deloitte.

Cyber Risks

What you don't know can hurt you

October 2014

Francophones and RATs
Do my ears deceive me?

- With trust, typically obtained by acting as an employee with impeccable local language, attackers gain access to computers, servers, systems, etc.
- Often, RATs (remote access Trojans) are utilized to gain valuable information and/or misappropriate assets
- Aggressive and sophisticated technics deployed for the first time in 2013

Example

- RAT gained access, attacker then obtained personnel info. and sensitive information including DRP/BCP plans
- Attacker called telecom provider, impersonating a company employee and convinced telecom provider to reroute all calls, as a result of a physical disaster, to “attacker-controlled” phones
- Attacker requested several large wire transfers from the bank via fax
- Calls by the bank to verify identity, etc. were routed to the “attacker-controlled” phones and, accordingly, wires executed

Discussion

- What is your company doing to ensure all employees are vigilant and risk intelligent/aware? What monitoring, behavioral analysis, or data analytics are being used to identify suspicious activity?

New York Times Hacked After on PM Jiabao Family

Can I believe what I read?

- October 2013 NY Times article links PM Wen Jiabao's family to intricate financial holdings
- Persistent and successful hacking attacks from China followed
- Company's antivirus software detected 1 of 46 malware tools

Approach

- Reporters emails read presumably an attempt to identify Chinese sources
- Sophisticated attacks routed thru US universities exploited by PLA in the past
- Tool signatures similar to tools attributed to past Chinese hacking groups
- Stole passwords and gained access to 43 employee personal computers
- Customized software designed and deployed to steal target reporters emails off email server
- Activities monitored for 4 months before shutdown
- NY Times warned by Chinese officials there would be consequences
- Other papers suffered similar attacks after publishing critical news

Malicious Insiders
Et tu, Brute?

- A current or former employee or contractor who deliberately exploited the network, system or data access to disrupt, embarrass or steal
- A recent study indicated that more than 50% of companies affected by malicious insiders stated that the damage caused by malicious insiders was greater than that by outsider attacks

Four common examples of malicious insider events:

- Theft of intellectual property
- Unauthorized access to / use of information, systems or networks
- Theft of other proprietary information (e.g., customer data, trade secrets, etc.)

Goldman Sachs and DuPont

- Accused former trader of stealing code related to a proprietary trading algorithm
- Market dominant positions challenged / threatened by smaller, competing firms by hiring former employees and paying for

Discussion

- Have you identified and secured your “crown jewel” data?
- Do you see this as a more or less significant threat to your organization?
- What other actions does your company take to prevent malicious acts by insiders (e.g., monitoring of large transfers / download of data)?

Lawsuits & Regulatory Actions

Growing risk of fines, class actions arising from data breach

- UK Information Commissioner authority to find up to £500,000 for breaches of Data Protection Act
- SEC Corporation Finance Guidance on Disclosing Cyber Risk
- Up to $500K per year in fines under strict Florida data breach law
- EU ramping up data privacy protections (new privacy directive)

250m user records stolen after Anonymous hacked Sony PlayStation servers

- 65 class action lawsuits filed, one settled for over $1m
- Though servers in California, UK Information Commissioner fined £250K
- Zurich refused to indemnify Sony under General Commercial Policy

Target hacked and data for 45m credit cards stolen

- SEC inquiry ongoing
- 100 class action lawsuits
- 2 directors sued in derivative lawsuits—implicating D&O coverage

Hackers steal 144m eBay user records

- UK Information Commissioner investigating US-based breach
- At least 4 states investigating
- Senate Commission holding inquiries

Cyber security

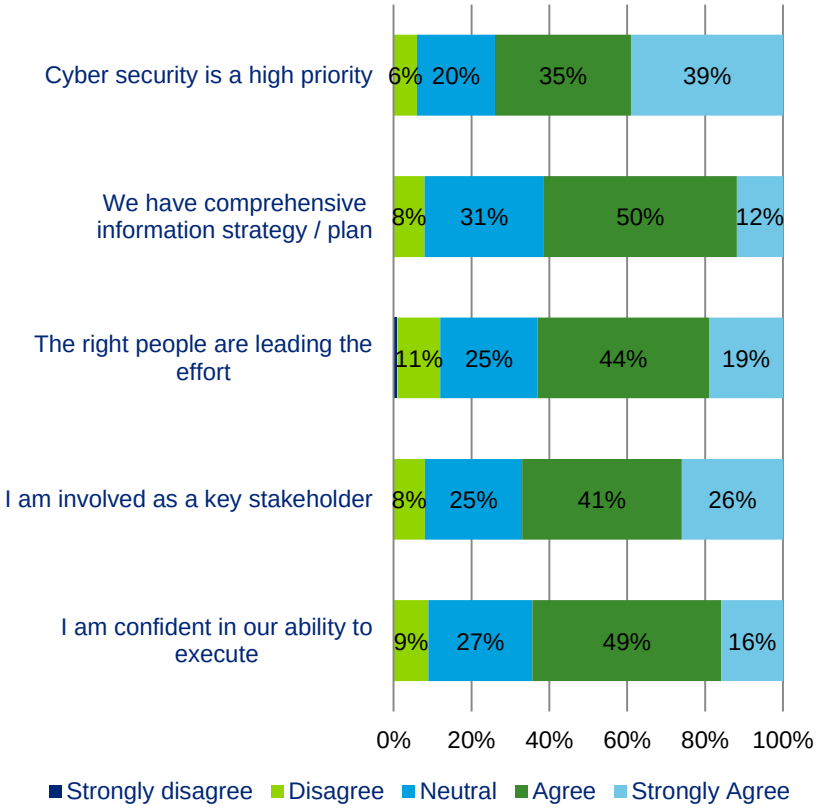
How do companies handle information security risks?

CFOs view cyber security as a high priority, but there are concerns about execution of information security plans.

- Cyber threats recognized: Overall, 74% of CFOs say cyber security is a top priority. This is particularly true among CFOs in Financial Services (92%) and Technology (90%). Only 6% (11% in Healthcare/Pharma) do not view cyber security as a high priority.
- Data protection plans in place: To combat cyber risks, 62% of CFOs say they have a comprehensive information strategy and plan in place. Financial Services CFOs are more likely than others to have one (93%), while Manufacturing CFOs are the least likely (40%). Twenty percent of Manufacturing CFOs say they do not have a plan in place.
- Right people involved, including the CFO: To 63% of CFOs, the right people are leading the cyber security effort at their companies. This is particularly true in Services (78%) and Financial Services (77%). As part of that effort, 67% of CFOs report being involved as a key stakeholder. This is most likely the case in Retail (86%) and Technology (80%). In Services, though, only 33% of CFO agree that they are involved as a key stakeholder, and no one strongly agrees.
- Not comfortable with ability to execute: Thirty-six percent of CFOs are not comfortable with their companies' ability to execute on their information security strategies. Retail CFOs (80%) express the most confidence in their companies' ability to execute, while T/M/E CFOs (22%).are the least confident.

How would you characterize your company's handling of information security risks?

- Percent of CFOs citing level of agreement with each statement (n=103)



Session Summary

Polling Questions

Q1. Do you educate your employees on spear phishing, social engineering and the risks related

n=9

Q2. Does your cyber security regime include a detection capability focused on identifying ongoing, successful intrusions?

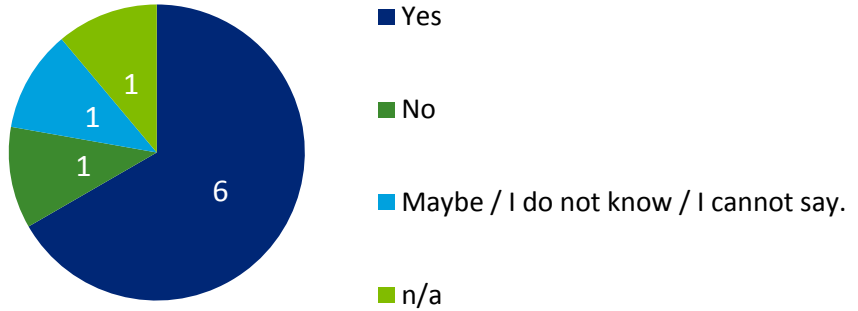
Q3. Do you have IT systems designed and implemented to help detect insider theft of trade secrets?

Polling Questions

Q4. Do you have a response plan in place for dealing with a data breach?

n=9

Q5. Does your response plan include dealing with regulators and third party legal claims arising from theft of your customer or third-party data?



Useful Links

Below are a few links that you may find useful

- Carnegie Mellon University's Computer Emergency Response Team (CERT)
  http://www.cert.org/
- Fortune “Your company is probably going to get hacked. Here's how to protect it” (Nina Easton, 24 October 2014)
  http://fortune.com/2014/10/24/hack-protection/?xid=nl_termsheet
- Fortune “Cybercrime is outwitting, outpacing security” (Robert Hackett, 28 May 2014)
  http://fortune.com/2014/05/28/cybercrime-is-outwitting-outpacing-security/
- Wired Business Media “Deloitte Brings Cyber War Games to the Enterprise”
  http://www.securityweek.com/deloitte-brings-cyber-war-games-enterprise
- CFO Insights “Cybersecurity: Five essential truths”
  http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/CFO_Center_FT/us_cfo_cybersecurity_073014.pdf

Contacts

Contacts

Deloitte

William (Bud) Roth

Senior Manager
Public Sector

+81 80 4651 5850
wroth@tohmatsu.co.jp

Scott Bower

Partner
Financial Industry Group

+81 90 3914 7007
scott.bower@tohmatsu.co.jp

Michael M. Laurer

Manager
The CFO Program | Japan

+81 80 4363 4814
mlaurer@tohmatsu.co.jp

Deloitte. トーマツ.

Deloitte Tohmatsu Consulting (DTC) is a Japan-based member firm of Deloitte -a worldwide network providing professional services and advice. As an entity in the Deloitte Touche Tohmatsu Limited providing four professional service areas: audit, tax, consulting, and financial advisory services, DTC provides consulting services in Japan and to Japanese companies worldwide. DTC's integrated services cover strategy through implementation to solve wide-ranging management challenges. DTC works closely with other Deloitte member firms both in Japan and overseas by leveraging the deep intellectual capital of approximately 200,000 professionals worldwide.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see http://www.deloitte.com/jp/en/about/ for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Member of
Deloitte Touche Tohmatsu Limited