Cyber Security Incident Response

Fighting Fire with Fire

Arun Perinkolam, Senior Manager

Deloitte & Touche LLP

Professional Techniques – T21

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

AGENDA

- Companies like yours
- What is the threat?
- What is the potential impact?
- What do leading practices look like?
- Staying ahead of the curve
- Appendix
- Q&A

COMPANIES LIKE YOURS

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Companies like yours …

Click on video

WHAT IS THE THREAT?

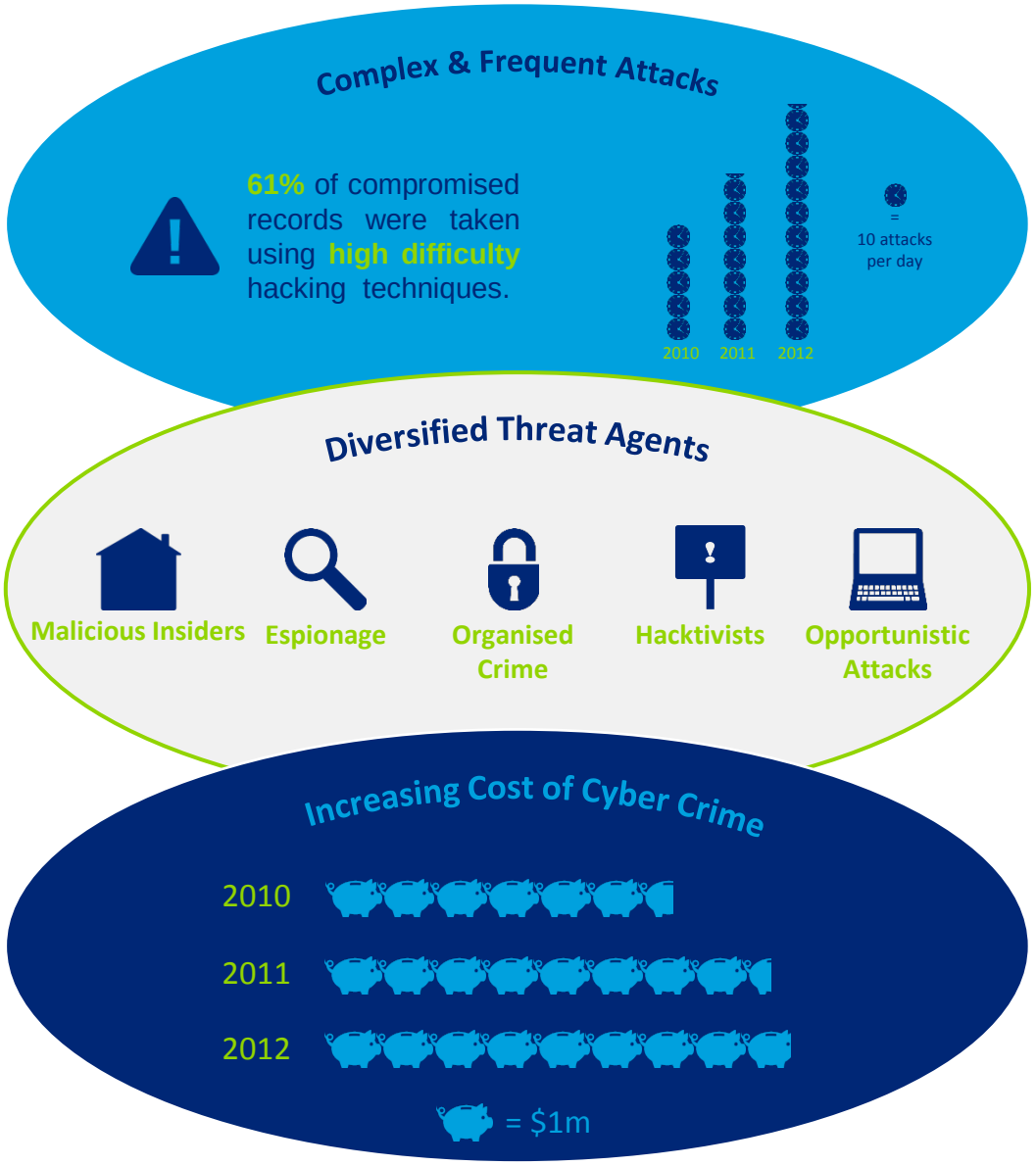
The advancing threat

The times they are a-changin'

The digital revolution is driving business innovation and growth, yet also exposing us to new and emerging threats.

The threat landscape is changing, and businesses have had to accept that it is not possible to prevent all forms of cyber attack, especially those that are particularly sophisticated and targeted.

The frequency of cyber attack is steadily increasing, and it only takes a single weakness for an attack to be successful.



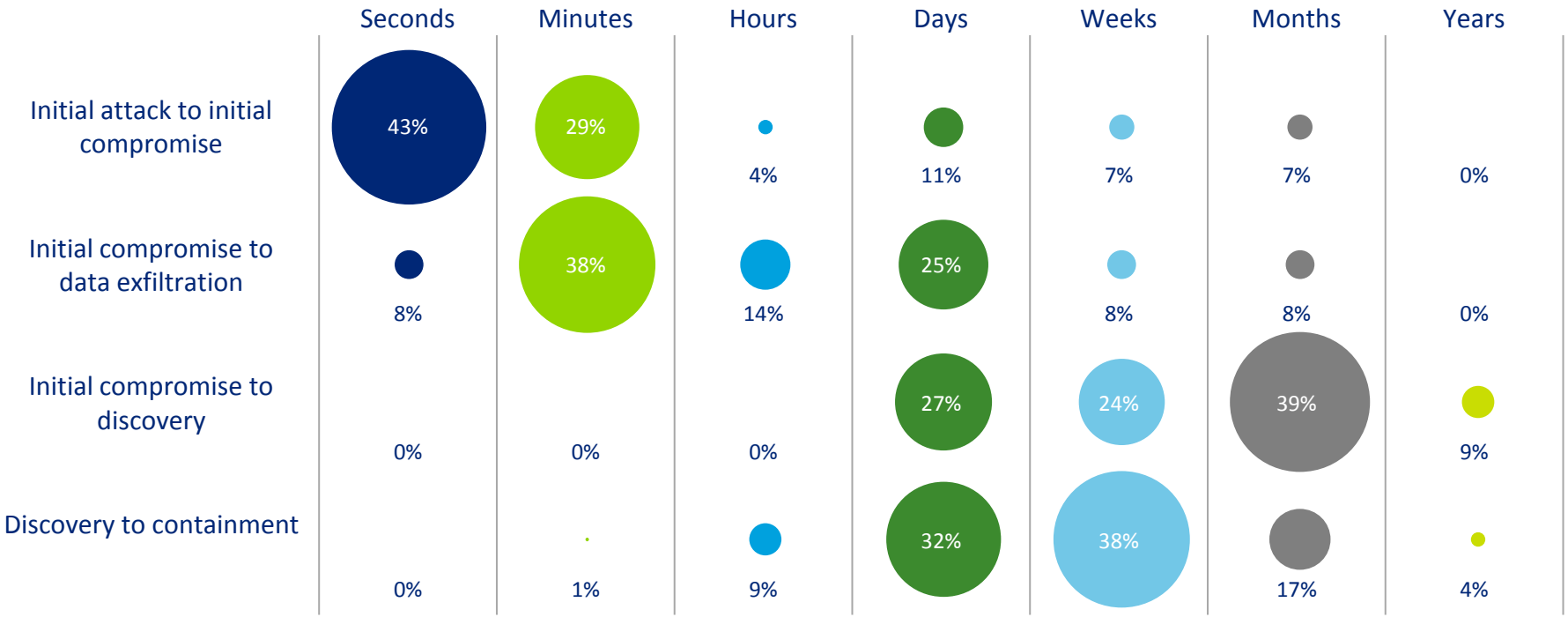
Data Sources: Verizon 2012 Data Breach investigations Report, Ponemon 2012 Cost of Cyber Crime Study

The advancing threat

The odds aren't in your favor

Attackers have a limitless number of attempts to compromise your defenses, but it only takes a single weakness on your part to get in.

It is an unfair game, but you can still prevent or significantly limit damage by quickly identifying and dealing with instances of compromise.



Data Source: Verizon 2012 Data Breach investigations Report

WHAT IS THE POTENTIAL IMPACT?

Consequences of an attack

- Financial losses and share price damage
- Brand and reputation
- Regulatory environment
- Costs of remediation and investigation
- Impact to operational capabilities
- Loss of intellectual property
- Risk to employees

Many organizations remain overconfident about their current level of security leaving them vulnerable to attack …

$110 billion

Estimated cost of cyber crime to U.S. economy[1]

88%

Of organizations surveyed are confident that they are protected against external cyber threats[2]

Yet …

59%

Of companies had knowingly experienced a security incident in the past 12 months[2]

[1]2012 Cybercrime Report, Symantec

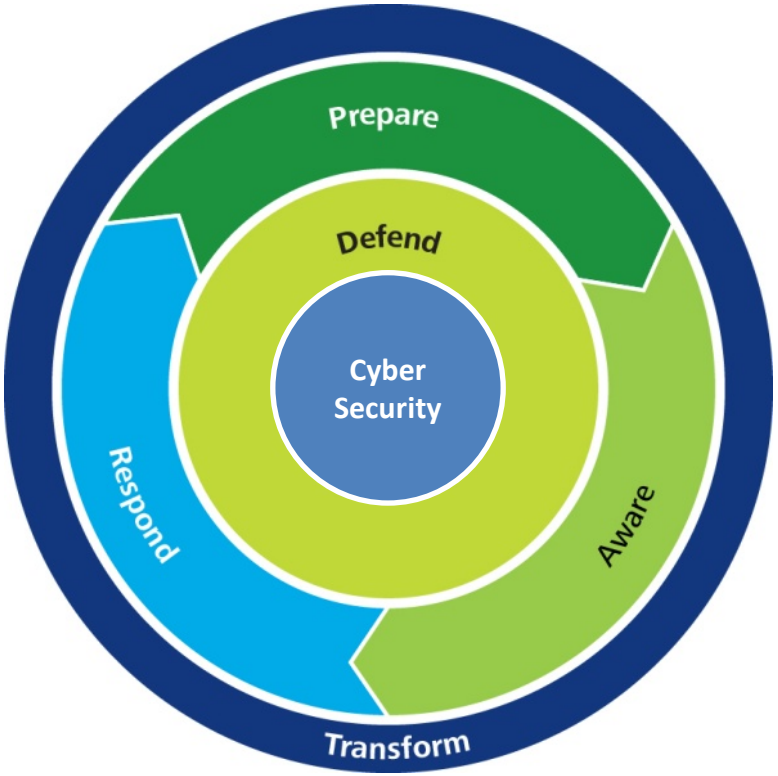
[2]2013 Deloitte TMT Global Security Study

WHAT DO LEADING PRACTICES LOOK LIKE?

Prepare, Be Aware, and Respond …

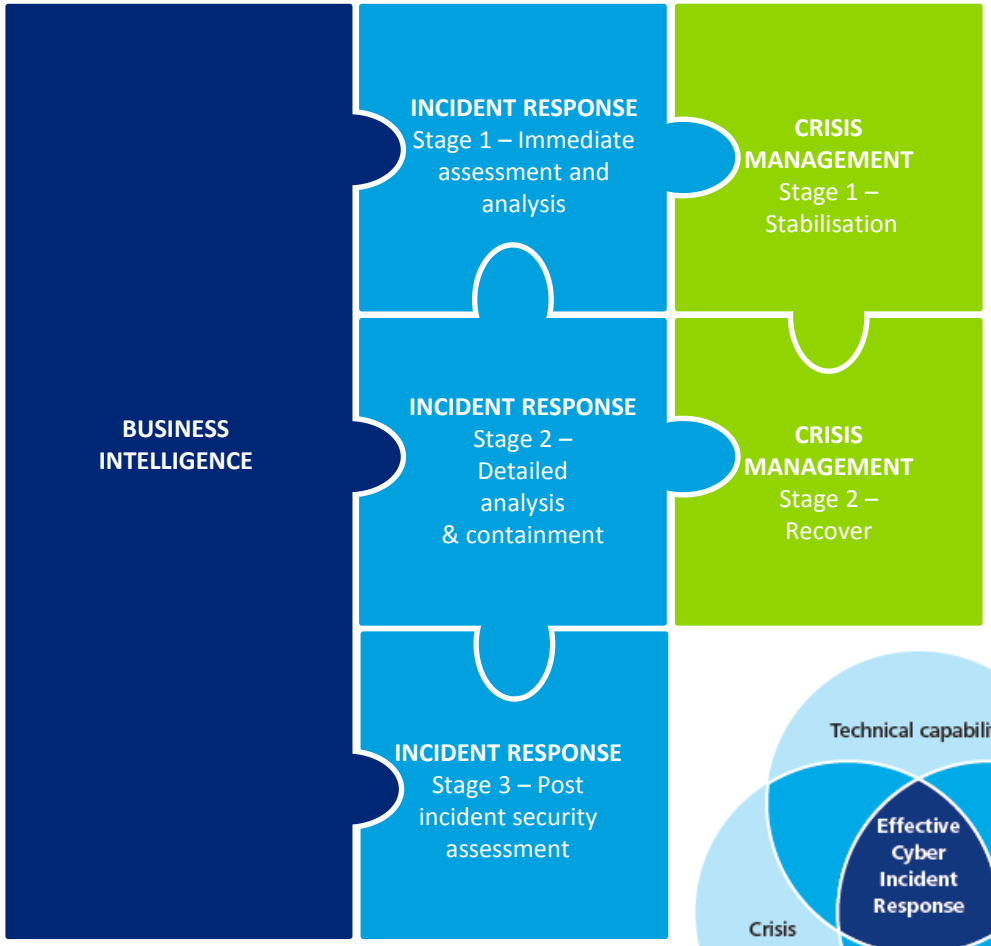
A leading practices response approach is founded on the following core principles:

- Be aware of their threat profile and vulnerabilities;
- Be prepared before an attack; and
- Respond effectively should an attack happen.



Effective Cyber Incident Response

- Manage and respond to high-consequence events which have the potential to seriously disrupt operations, damage reputation and destroy shareholder value
- Conduct technical and forensic analysis of incidents
- Assess incident and support containment / minimization of damage
- Execute technical incident response
- Manage public relations
- Manage internal communications and reporting



Using Business Intelligence

How would a potential global contagion impact us?

How would a significant redistribution of resources impact business as usual?

Can we manage the disconnect between the pervasiveness of rumour fuelled by social media and our ability to respond based on fact?

How can we ensure our message is consistent from an internal and external perspective?

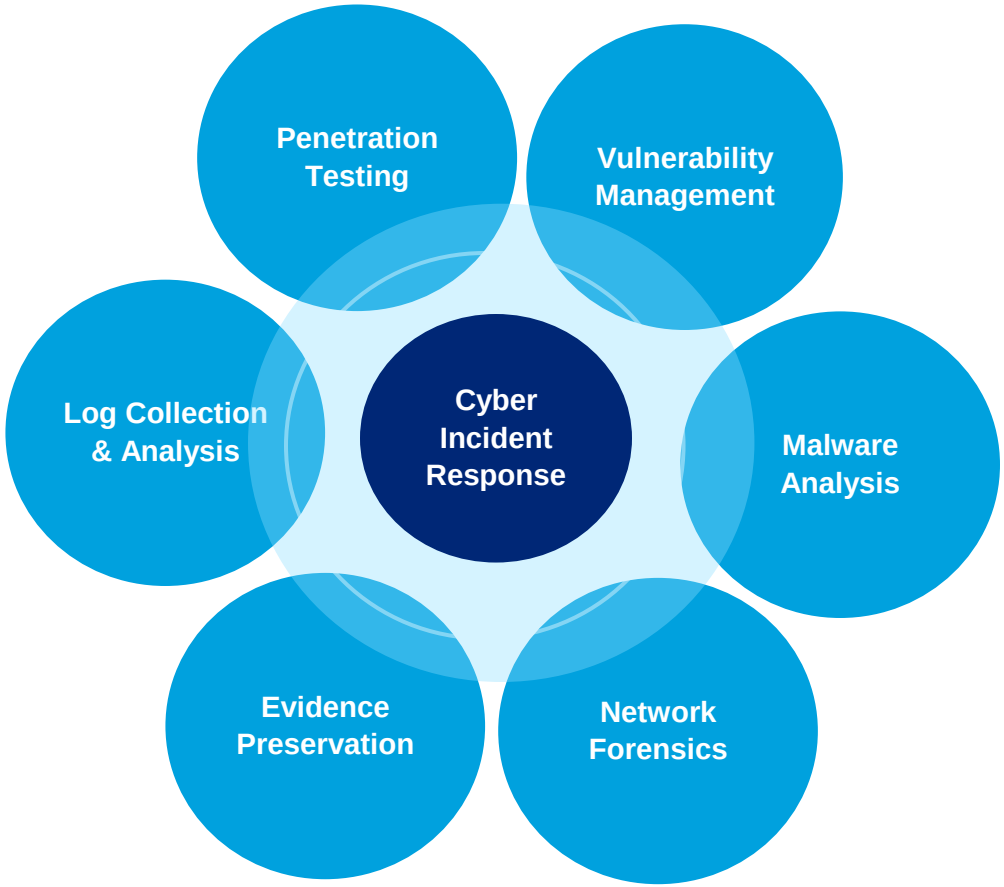
How can we move from a reactive to proactive stance to more effectively understand the cyber threat?

What is the worst case scenario and what technical measures can we take to limit the impact without significantly damaging the business?

Leveraging Supporting Capabilities

Supporting Capabilities

- Cyber Security Education
- Insider Threat Detection
- Cyber Security Readiness Assessment
- Solution Research and Development
- Application Security Review



Supporting Capabilities

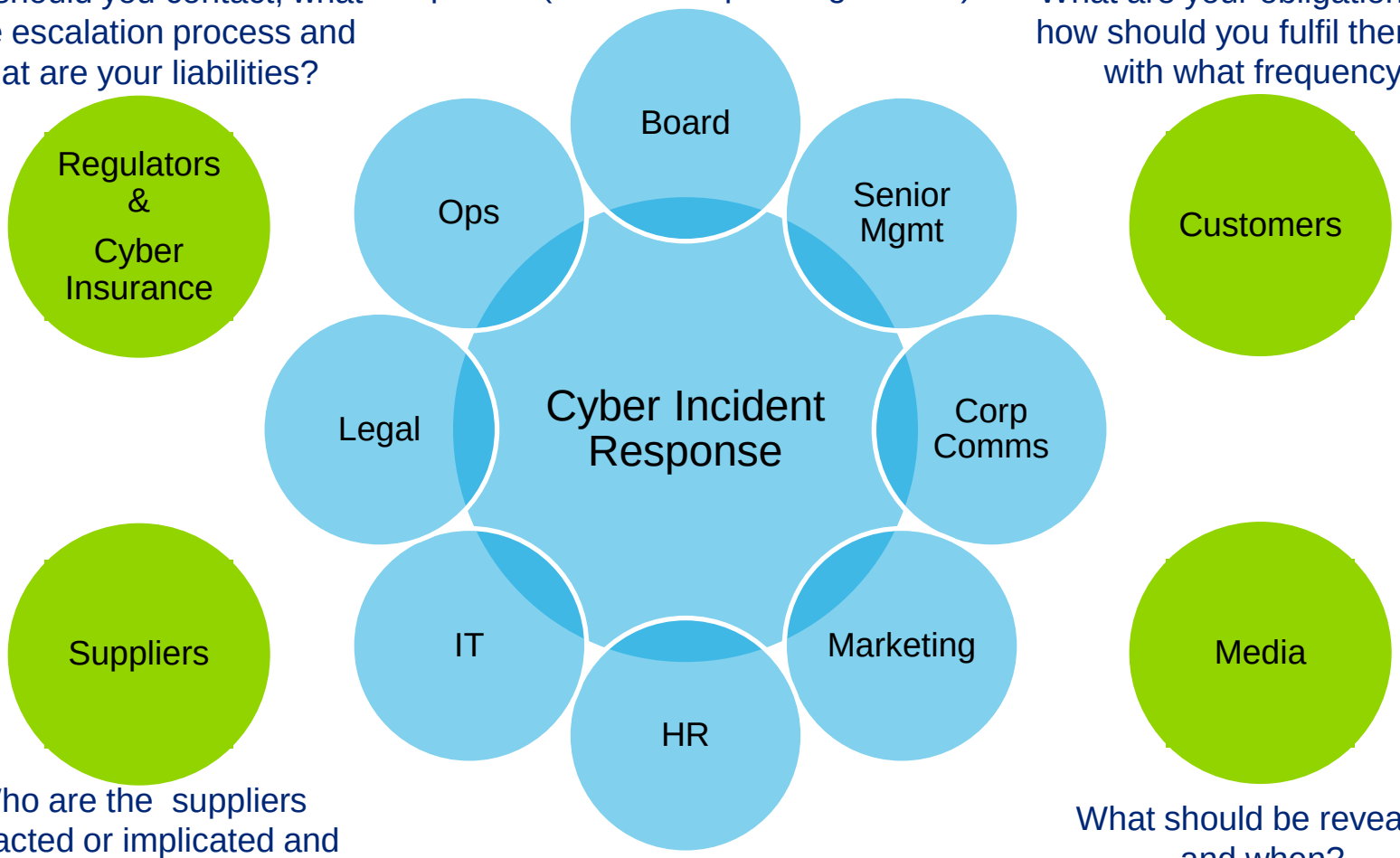
- Cyber Threat Modeling
- Third Party Threat Monitoring
- Identity and Access Management
- Brand Monitoring
- Cyber Threat Intelligence

Effective Crisis Management

How do you establish a single source of authorised information and intelligence picture (Common Operating Picture)?

Who should you contact, what is the escalation process and what are your liabilities?

What are your obligations and how should you fulfil them and with what frequency?



Who are the suppliers impacted or implicated and how best to coordinate?

What should be revealed and when?

STAYING AHEAD OF THE CURVE

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Build an effective CIR program - Preparation

A mature, leading practices based Cyber Incident response (CIR) program typically has formality with regard to IR preparation, collection and analysis, communication and post-incident investigation.

KEY ACTIVITIES

- Define incident handling team organization
- Confirm sign off authority and thresholds for response
- Document security procedures and methods to exchange information
- Identify support teams and team facilitators at all levels
- Identify individuals who can be quickly deployed
- Implement incident reporting mechanisms

Build an effective CIR program - Collection, analysis and preservation

A mature, leading practices-based CIR program typically has formality with regard to IR preparation, collection and analysis, communication and post-incident investigation.

KEY ACTIVITIES

- Detect, capture and analyze network traffic and system data
- Create backups and isolate potentially compromised systems
- Identify, capture and analyze pertinent files within compromised local systems and other data sources
- Reconstruct sequence of events on compromised systems
- Identify additional investigative steps based on initial analysis
- Securely preserve and maintain data gathered
- Generate secure backups of data and evidence collected
- Preserve the chain of custody
- Document approach and steps taken to collect and analyze evidence
- Document output and key findings from evidence analysis
- Provide interim report on analysis of evidence and provide preliminary conclusions

Build an effective CIR program - Communication

A mature, leading practices-based CIR program typically has formality with regard to IR preparation, collection and analysis, communication and post-incident investigation.

KEY ACTIVITIES

- Inform organization on progress of incident response
- Inform all parties affected by the incident in a secure manner
- Establish media and Internet monitoring
- Notify upstream and downstream parties, such as Internet Service Providers, and other service providers in a secure manner
- Maintain stakeholder contact lists and logs
- Consider informing the police/regulators

Build an effective CIR program - Post-incident Activities

A mature, leading practices-based CIR program typically has formality with regard to IR preparation, collection and analysis, communication and post-incident investigation.

KEY ACTIVITIES

Containment
- Contain incident and minimize immediate damage
- Apply technical and administrative solutions to mitigate risk of further exposure
- Assess cause and symptoms of incident and eradicate any remaining attacker artifacts

Recovery and record
- Prioritize recovery activities to support the return to business as usual
- Issue formal report detailing the incident response process and providing recommendations for remediation
- Hold “lessons learned” meeting with all involved parties

Prevention
- Correct systemic weaknesses and deficiencies by revising security plans and policies
- Advise on technical and administrative solutions in order to minimize risk of future cyber incidents
- Monitoring to determine effectiveness of response measures

APPENDIX

About Deloitte's Security & Privacy Services

At Deloitte, our security and IT risk consulting services are independently recognised as world leading.

Our people

At Deloitte in the U.S., and globally through the Deloitte Touche Tohmatsu Limited network of member firms, our global team can draw on the experience of;

- >4500 professionals in North America and over 11,000 risk management and security, privacy and resilience practitioners globally
- 210 computer forensics examiners, part of Deloitte Financial Advisory Services LLP
- 11,530 human capital consulting professionals, part of Deloitte Consulting LLP

Our skills

- ✓ **ISACA:** Over 8,000 involved with ISACA; approximately 2,000 certified as CISA, CISM, & CGEIT
- ✓ **ISC²:** Over 1,100 CISSPs
- ✓ **BSI:** 150 trained lead system auditors
- ✓ **IAPP:** Privacy certified practitioners
- ✓ **PMI:** PMP certified practitioners

53 Security & Forensics labs located strategically across the globe

Q & A

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.