DUFF & PHELPS

Penetration Testing and Scenario Exercising

James Weare
Trevor Dickey

June 12 2017

Presenters

James Weare, CISSP

Vice President, Information Security

james.weare@duffandphelps.com

- 7 years industry experience in Security Operations, Audit, and Infrastructure
- Background in Financial Services & Capital Markets
- Experienced pen tester and cyber incident responder

Trevor Dickey, CFCE

Vice President, Forensic Technology

trevor.dickey@duffandphelps.com

- Veteran of law enforcement with 16 years of experience
- Met Police e-Crime Unit & National Hi-Tech Crime Unit
- Subject Matter Expert in Cyber Crime Investigations

Table of Contents

- Information Security Basics
- Existing & Future Legislation
- Top 5 Real & Perceived Risks in Information Security
- Cost of Data Breaches and Ransomware
- Defining Security Measures
    - SANS Critical Controls
    - Incident Response
    - Penetration Testing
- The Role of Cyber Insurance
- Case Studies
    - Incident Response Planning Case Study
    - Former Employee Data Exfiltration, March 2017
    - WannaCry Ransomware Incident, May 2017
- Workshop: Group Incident Response Exercise

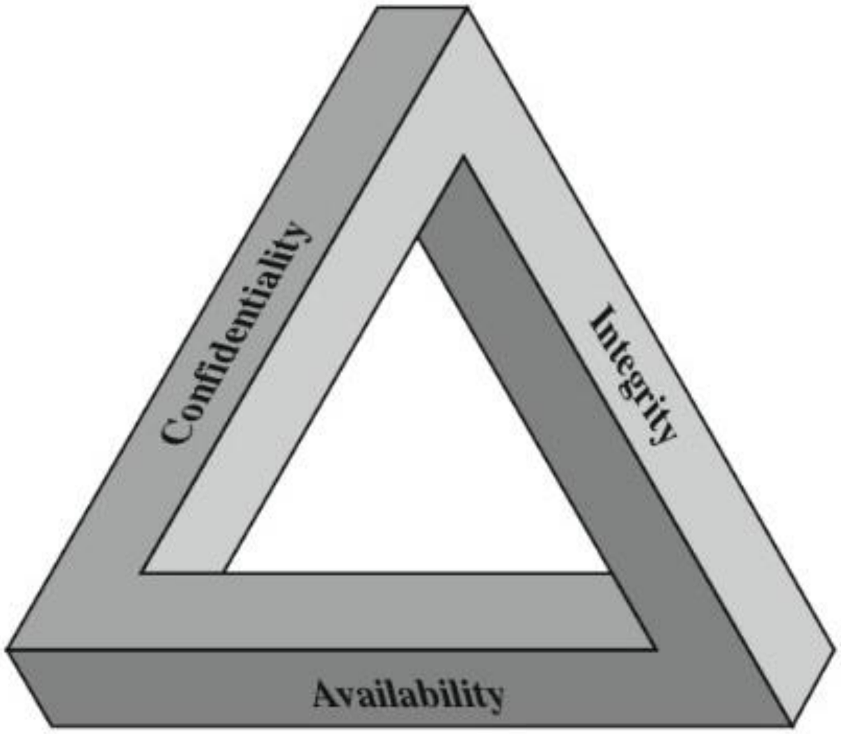
Information Security Basics

3 security principles for data:

- Confidentiality
- Integrity
- Availability

Each principle has its own risks:

- Confidentiality: data breach/disclosure
- Integrity: data alteration or partial destruction
- Availability: total data destruction, ransomware, DDoS



Legislation, Then and Now

Then: UK Data Protection Act, 1997

- Maximum fines of £500k/1% annual turnover
- No breach reporting obligation
- No right to erasure
- No Privacy Impact Assessment requirements
- Consent for data collection can be opt-in or opt-out

Legislation, Then and Now

Now: EU General Data Protection Regulation

- Comes into effect May 25, 2018
- Significantly increased fines:
  - €20MM or 4% annual turnover for violations related to consent, data subject’s rights
  - €10MM or 2% global turnover for failure to implement sufficient control measures, records maintenance, breach reporting
- 72 hour window to report a data breach
- Right to erasure provision
- Privacy assessment to determine impact to data subjects
- Revocable, opt-in consent

Cybersecurity Risks

Question:

What are your top 5 perceived cybersecurity risks?

According to a United Service Providers study in 2016:

- Insider Threats & Social Engineering
- Malware/Ransomware
- Cloud Computing
- Mobile Technology
- Skills Shortages

Assessing the Risks

Insider Threats & Social Engineering

- Access to proprietary data can be exploited for financial gain
- Phishing & spear phishing, vishing, smishing
- I just found this USB stick out in the parking lot…

Malware/Ransomware

- Difficulty of prevention (0-days, the human element)
- Costly to clean up
- Inconsistent backup regimens

Cloud Computing

- Microsoft Azure, Amazon AWS
- New “fuzzy” perimeter presents challenges for traditional IT teams
- Where is my data? – easier to answer than you think

Assessing the Risks, continued

Mobile Computing

- Smartphones, tablets, laptops, oh my!
- How do we protect the data on these devices?

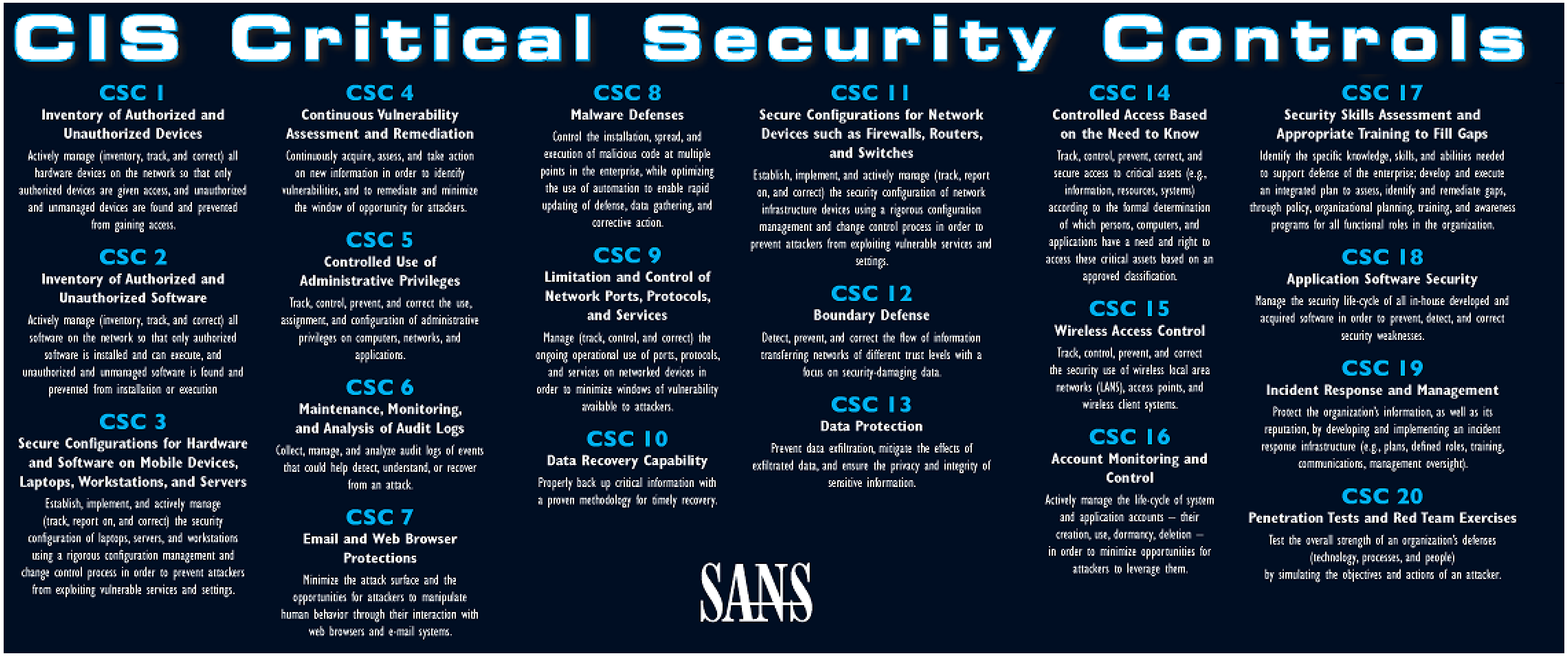
Skills Shortages

- US Bureau of Labour Statistics: 209k unfilled cybersecurity jobs
- Cisco: 6MM cybersecurity jobs globally by 2019
- Symantec: Projected shortfall of 1.5MM by 2019

Defining Security Measures

SANS Critical Security Controls cover:

- Information Systems Inventories
- Configuration Management
- Vulnerability Assessments and Penetration Testing
- Access Controls
- Incident Response and Incident Management



CIS Critical Security Controls

CSC 1
Inventory of Authorized and Unauthorized Devices
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CSC 2
Inventory of Authorized and Unauthorized Software
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution

CSC 3
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 4
Continuous Vulnerability Assessment and Remediation
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5
Controlled Use of Administrative Privileges
Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6
Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7
Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems.

CSC 8
Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9
Limitation and Control of Network Ports, Protocols, and Services
Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10
Data Recovery Capability
Properly back up critical information with a proven methodology for timely recovery.

CSC 11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12
Boundary Defense
Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CSC 13
Data Protection
Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

SANS

CSC 14
Controlled Access Based on the Need to Know
Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 15
Wireless Access Control
Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16
Account Monitoring and Control
Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17
Security Skills Assessment and Appropriate Training to Fill Gaps
Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18
Application Software Security
Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

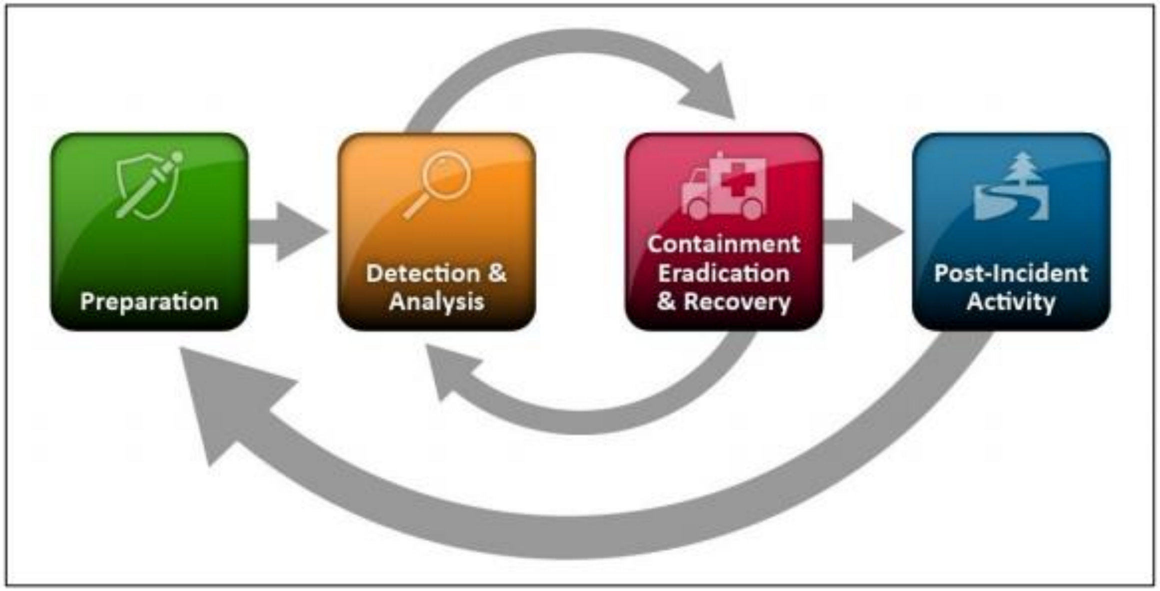
CSC 19
Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20
Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

Incident Response

A successful incident response and management approach includes:

- Defined plans
- Assigned roles
- Training and review
- Communications management
- Executive oversight and involvement
- Continuous feedback



Source: NIST 800-61 Revision 2

Penetration Testing

Vulnerability Assessment

- Analyzes the information systems environment
- Reports on gaps in an organization’s technical security program

Penetration Testing

- Encompasses the information gathering element of a vulnerability assessment
- Actively exploits gaps in the security infrastructure to attempt a compromise
- Tests technical security measures as well as incident response measures and other established procedures

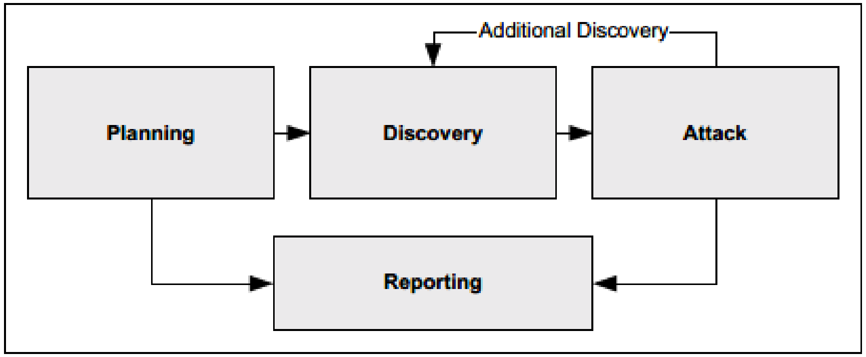


Figure 5-1. Four-Stage Penetration Testing Methodology

Source: NIST 800-115

Costs of Data Breaches and Ransomware

How much does a cyber incident cost?

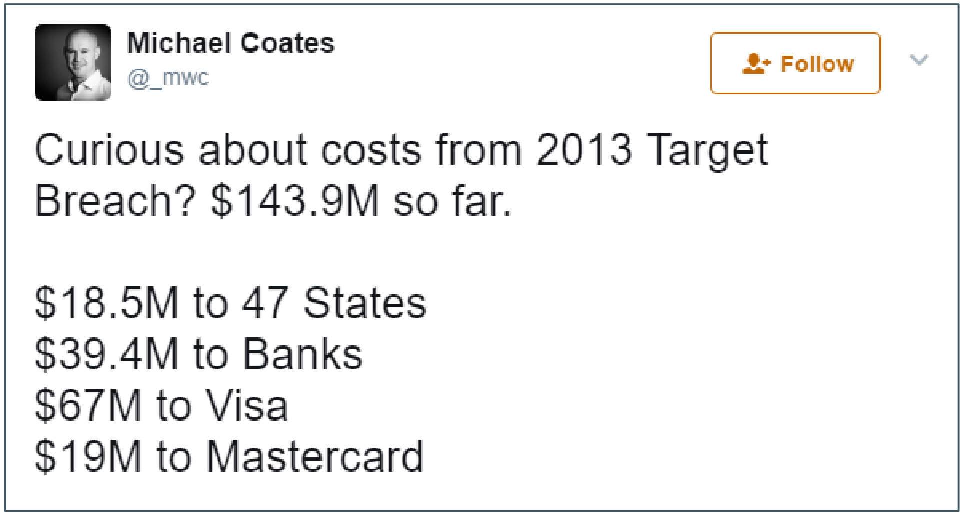
- Ponemon study:
  - $4MM USD/breach
  - $129-$355 USD/record (reduced by $16/record when having an IR team)
- Target breach

But... this number is hard to estimate!

- Differing regulatory regimes
- Cost of containment? Fines? Cleanup? Remediation? etc.

Ransomware: When do we pay up?

- Often involve small sums (US$500)
- Is there any guarantee an attacker will actually unlock files?



Michael Coates
@_mwc

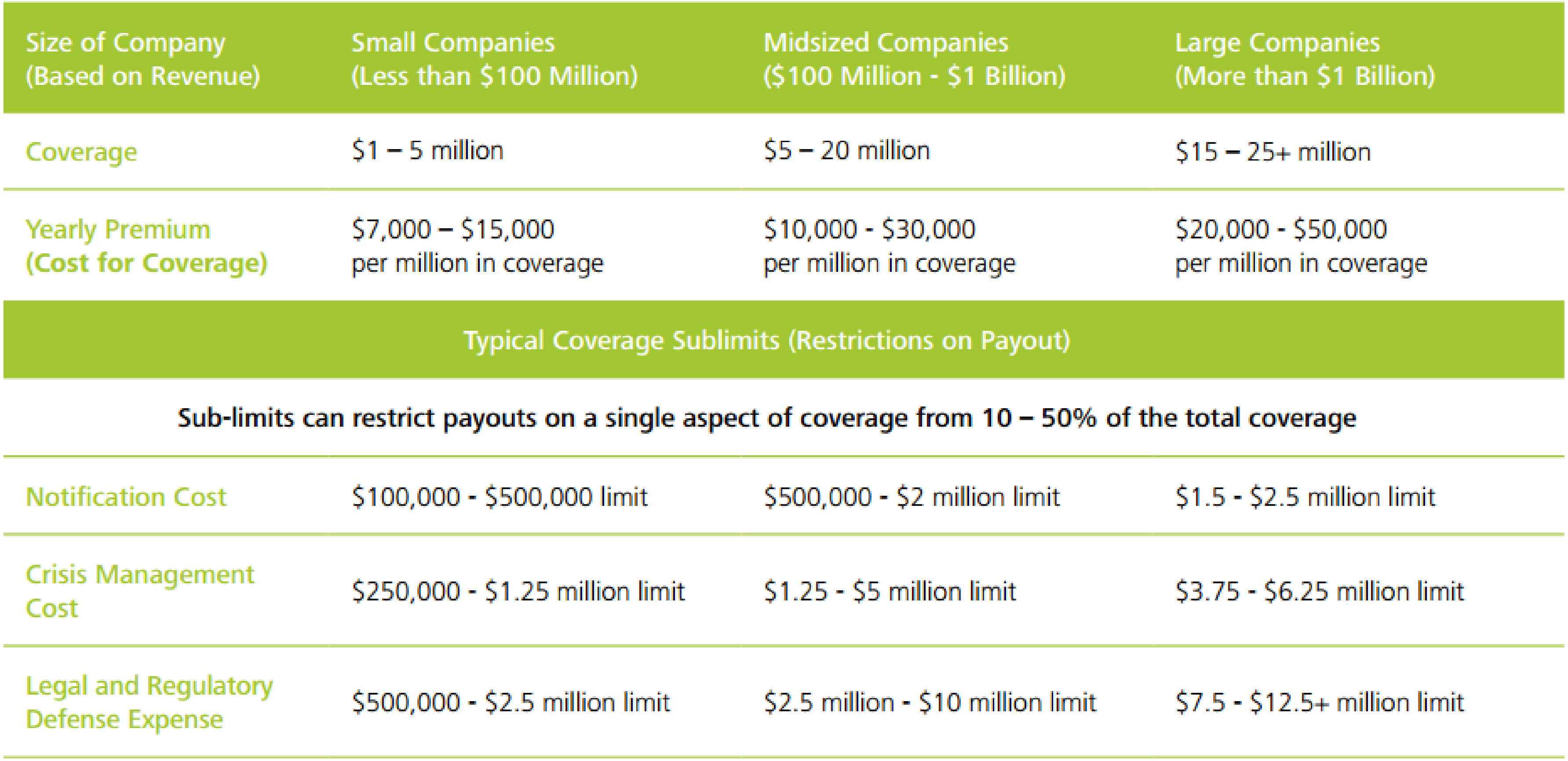
Curious about costs from 2013 Target Breach? $143.9M so far.

$18.5M to 47 States
$39.4M to Banks
$67M to Visa
$19M to Mastercard

The Role of Cyber Insurance

- Assist in recovery of costs associated with management, communication, recovery of a cyber incident
- May already be covered by existing policy
  - Though many policies have exclusions for cyber!
- Many insurers offering cyber policies have partners who can assist with incident response
- Cost of a breach can be extremely high; insurance can cover or at least offset this cost
- Can be an important part of an Incident Response plan

Typical Cyber Insurance Premiums



Size of Company (Based on Revenue)	Small Companies (Less than $100 Million)	Midsized Companies ($100 Million - $1 Billion)	Large Companies (More than $1 Billion)
Coverage	$1 – 5 million	$5 – 20 million	$15 – 25+ million
Yearly Premium **(Cost for Coverage)**	$7,000 – $15,000 per million in coverage	$10,000 - $30,000 per million in coverage	$20,000 - $50,000 per million in coverage
Typical Coverage Sublimits (Restrictions on Payout)			
Sub-limits can restrict payouts on a single aspect of coverage from 10 – 50% of the total coverage			
Notification Cost	$100,000 - $500,000 limit	$500,000 - $2 million limit	$1.5 - $2.5 million limit
Crisis Management Cost	$250,000 - $1.25 million limit	$1.25 - $5 million limit	$3.75 - $6.25 million limit
Legal and Regulatory Defense Expense	$500,000 - $2.5 million limit	$2.5 million - $10 million limit	$7.5 - $12.5+ million limit

Source: Deloitte

Case Studies

Case 1: Preparation/Incident Response Planning Case Study

- Hedge fund COO meeting with investor
- Investor inquired about Incident Response plan testing
- COO replied that there was a recent breach:
  - Via breach response experience, IR plan was executed, changes documented, clean-up performed.
  - Success story! (Is it?)

- ODD team inquired if IRP had been **tested**:
  - No table top exercises ever performed
  - No run-through of incident response steps via penetration test
  - Breach response “success” was really just luck
  - Very embarrassing for COO

- Hedge fund was eventually funded:
  - IR plan was required to be regularly tested and updated

Case Studies, continued

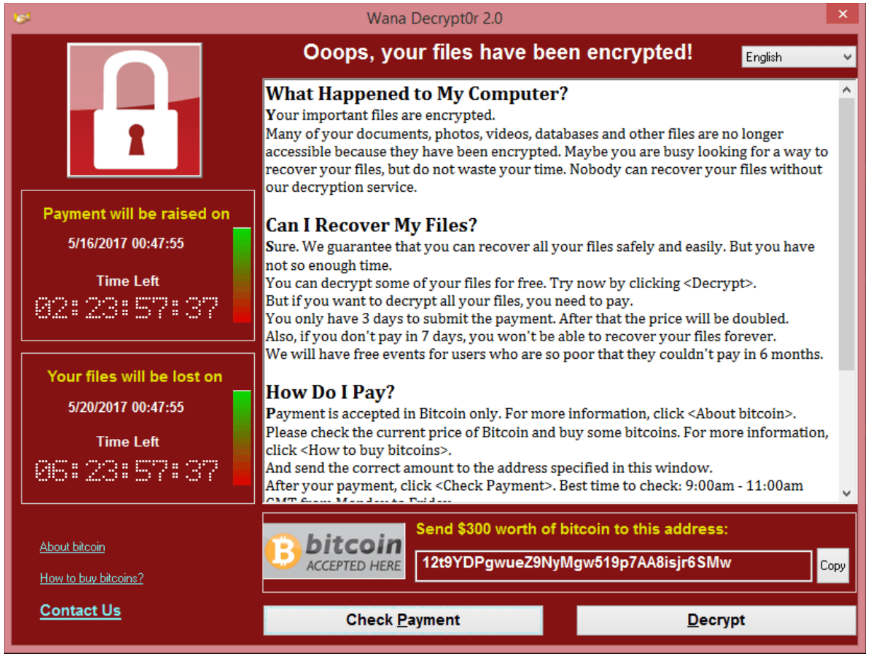
Case 2: Data exfiltrated by former employee

- Employee had submitted their notice of departure
  - Non-compete clause in place
  - Employee was moving on to a competitor
- Employee's system was searched for evidence of data leakage
  - Evidence of upload to cloud storage provide found
- Open Source Intelligence (OSINT) showed that employee had posted on social media
  - "I'm downloading a large amount of data from cloud storage… taking forever!"
- Evidence was likely used in order to enforce compliance with non-compete clause

Case Studies, continued

Case 3: WannaCry Ransomware Attack

- Encrypts documents and requires a ransom to unlock them
- Initial injection vector was a poorly-configured/Internet exposed service
- Propagates using NSA-developed exploits abusing previously unknown flaws in Microsoft Windows SMB protocol
- Uses “kill switch” domain to determine if it should execute
- US DHS advises not to pay ransom to attackers
- Attribution difficult, but likely points to North Korean origin



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Case Study 3

Cleanup:

- Disconnect all affected systems from network
- Disable/block related network traffic and update technical security policies
- Patch unaffected/vulnerable systems
- Re-image affected systems
- Restore from backup
  - What if we don’t have backups? Painful lesson learned!

Audience Exercise: Incident Response

- 4 groups, 1 scenario per group
- Walk through detection, triage, evidence gathering, mitigation/containment, eradication, recovery
- Discuss what was expected, unexpected, lessons learned

Final Q&As

DUFF & PHELPS

For more information about our global locations and services, please visit:
www.duffandphelps.com

About Duff & Phelps

Duff & Phelps is the premier global valuation and corporate finance advisor with expertise in complex valuation, dispute and legal management consulting, M&A, restructuring, and compliance and regulatory consulting. The firm's more than 2,000 employees serve a diverse range of clients from offices around the world. For more information, visit www.duffandphelps.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory and capital raising advisory services are provided in a number of European countries through Duff & Phelps Securities Ltd, UK, which includes branches in Ireland and Germany. Duff & Phelps Securities Ltd, UK, is regulated by the Financial Conduct Authority.