

Surviving a Security Breach

Kevin Wheeler, CISSP, CISA

www.infodefense.com

InfoDefense
Strategic Information Security

Security Breach Statistics

- Since June 2005, over 517 Million U.S. resident's data records have been exposed due to security breaches
Source: Privacy Rights Clearinghouse
- In 2009 the number of data security breaches increased by 46%. Source: Identity Theft Resource Center
- 44 states, the District of Columbia, Puerto Rico and US Virgin Islands have enacted security breach notification laws to help address the identity theft problem
- The average security breach costs an organization \$204 per lost record
Source: 2010 Annual Study: Cost of a Data Breach, Ponemon Institute, LLC


www.infodefense.com

InfoDefense
Strategic Information Security

Who is at Risk?

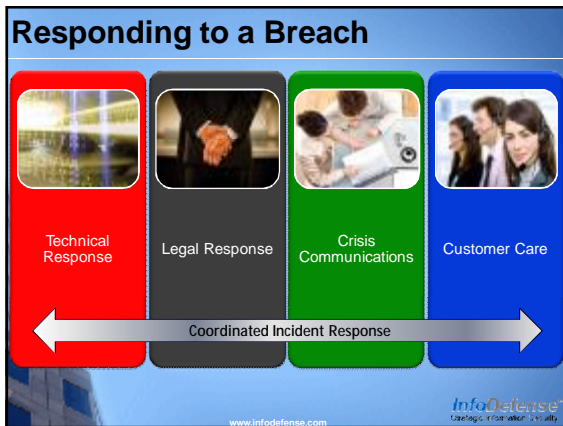
Organizations that...

- § Process credit cards, retain personal information or possess otherwise sensitive information
- § Own or possess intellectual property
- § Perform national security functions
- § Provide a "Critical Infrastructure" function



www.infodefense.com

InfoDefense
Strategic Information Security



Technical Response

- Cyber Attack
- Malware Outbreak
- Other Types of Breaches

InfoDefense
Strategic Information Security

www.infodefense.com

Cyber Attack

- Enable verbose logging
- If necessary, unplug the network cable to the system(s), but **DO NOT POWER THEM DOWN**
- Protect Evidence
- Contact a computer incident response expert and law enforcement
- Identify the information that may have been stolen and the customers, if any, that could be adversely affected
- Perform a root cause analysis

InfoDefense
Strategic Information Security

www.infodefense.com

Malware Outbreak (SEP Environments)

1. If not already enabled, turn on:
 - Bloodhound level 3
 - Client intrusion prevention
 - Client firewall
 - Network auto-protect
 - Deploy AV signature at the highest possible frequency
2. Enable granular logging on:
 - § Network devices
 - § Critical servers
 - § Other key systems
3. Contact Symantec Support
4. Remove infected systems from network (if necessary)

Americas
+ 1 800 634 4747
EMEA
+ 44 870 606 6000
Asia Pacific/Japan
+ 61 282 207 111

InfoDefense
Strategic Information Security

www.infodefense.com

Malware Outbreak (SEP Environments)

5. Capture suspicious files
 - § New malware should always be submitted to Security Response for analysis.
 - § Heuristic AV detection reports
 - § IPS signature alerts
 - § Load point analysis tool from technical support
 - § Gathers information on system load points to help identify possible malware
 - § <http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008053012231648?Open&seg=ent>
 - § Free tools that allow low-level access to file system
 - § Needed when the files in question can't be accessed via normal methods
 - § IceSword: <http://www.antirootkit.com/software/IceSword.htm>
 - § Bart's PE: <http://www.nu2.nu/pebuilder/>
 - § Attach infected drive to another system

InfoDefense
Strategic Information Security

www.infodefense.com

Malware Outbreak (SEP Environments)

6. Submit files
 - § Threat submission pages (slides 25 – 26)
 - § Threat Expert - <http://www.threatexpert.com/>
 - § Provides automated basic analysis of submitted file within one hour
7. Block suspicious files via SEP Application Control rule
 - § Use MD5 hash for each submitted file



InfoDefense
Strategic Information Security

www.infodefense.com

Malware Outbreak (SEP Environments)

[illegible]

Malware Outbreak (SEP Environments)

8. Deploy updated AV signatures
 - § Rapid Release package can be deployed to a SEPM server
 - § The customer can also wait for the next certified release through LiveUpdate
9. Use removal tools when needed
 - § http://www.symantec.com/orton/security_response/removaltools.jsp
 - § All tools have a silent mode to allow for command line execution
 - § All tools have a '/?' command line option to display all available options
10. Initiate a full scan of the system once new signatures are deployed
11. Only return the affected systems to the network after cleaning.

www.infodefense.com

InfoDefense
Cyberlogic. Not a word. A world.

Other Types of Breaches

- Identify the information that may have been stolen and the customers, if any, that could be adversely affected
- Contact your computer incident response expert and law enforcement
- Perform a root cause analysis

www.infodefense.com

InfoDefense
Creating Trust with Technology

Business Response

- Legal
- Crisis Communications
- Customer Care

www.infodefense.com

InfoDefense®
Strategic Information Security

Legal Response

- If the breach involves a customer's sensitive information, consider hiring an attorney that specializes in computer law
- Ensure that customers are notified in a timely manner
- Demonstrate a true concern for the customer. Allocate appropriate resources to field customer calls
- If the breach puts the customer at risk for identity theft, consider paying for credit monitoring services for a period of time

www.infodefense.com

InfoDefense®
Strategic Information Security

Crisis Communications

- Consider bringing in a crisis communications expert
- Inform key employees, but instruct them to not discuss the incident with anyone
- Set up a toll-free number for customers to call
- If legal counsel determines that notification is required by law, hold a press conference to inform potential victims of the breach
- If required, hold periodic press conferences.
- Notify customers that may be affected by the breach

www.infodefense.com

InfoDefense®
Strategic Information Security

Customer Care

- If the number of people affected by the breach will overwhelm your internal staff, consider using a customer care services such as those available from Trans Union, Equifax or Experian.
- Ensure that customers are notified of the breach in a timely manner
- If the breach puts the customer at risk for identity theft, consider paying for credit monitoring services for a period of time
- To the extent possible, make management available to answer customer concerns

www.infodefense.com

InfoDefense
Strategic Information Security

Preparing for a Breach

www.infodefense.com

InfoDefense
Strategic Information Security

Preparing for a Security Breach

1. Inform senior management about the risk of a security breach
2. Demonstrate “**Due Care**”
3. Create a computer incident response plan
4. Organize response teams
5. Develop relationships with law enforcement and subject matter experts

www.infodefense.com

InfoDefense
Strategic Information Security

Inform Senior Management

- Identify the existence of credit card, personally identifiable or other sensitive information within your organization
- Develop high-level security breach scenarios (i.e. lost or stolen laptops, lost backup tapes, system intrusion, etc.)
- Determine the potential financial, legal and public perception impact of each scenario

Demonstrate “Due Care”

- Perform a risk analysis to determine the potential impact of a breach
- Delete sensitive information that is no longer required
- Have a third-party expert perform a security assessment periodically
- Address known security issues (prioritize by risk)

Demonstrate “Due Care” cont.

- Ensure that the IT function is appropriately governed, that systems are updated periodically and that appropriate controls are in place
- Configure appropriate levels of system logging
- Install an intrusion prevention system to protect critical information

Computer Incident Response Plan

- Detailed technical response procedures for likely scenarios
- High-level crisis communications procedures
- Legal response guidelines
- Customer care guidelines and procedures including remediation services
- Contact information for all key vendors and response team members

www.infodefense.com

InfoDefense®
Strategic Information Security

Organize Response Teams

- Technical response
- Crisis communications
- Legal response
- Customer care

www.infodefense.com

InfoDefense®
Strategic Information Security

Develop Relationships

- Computer incident response and forensic experts
- Strategic security vendors
- Crisis communications/public relations experts
- Legal counsel with computer security law expertise
- Law enforcement (US Secret Service, FBI)
- Credit reporting agencies

www.infodefense.com

InfoDefense®
Strategic Information Security

How Can Symantec Help?

- Cyber attack breach response and remediation support
- Malware outbreak response
- Actionable threat information
- Information Risk Assessment
- Malicious Activity Assessment

www.infodefense.com

InfoDefense
Strategic Information Security

About InfoDefense

§ InfoDefense was founded in 2001 by information security industry experts and offers a comprehensive suite of information security services including:

- § Security Audit and Assessment
- § Regulatory Compliance
- § Strategic Security Planning and Policy Development
- § Security Architecture and Engineering
- § Computer Incident Response
- § Computer Forensics and Expert Witness
- § IT Security and Audit Training

§ Authored Works include **IT Auditing: Using Controls to Protect Information Assets** McGraw-Hill, 2006, 2nd Ed. 2010

www.infodefense.com

(877) INFODEFENSE

www.infodefense.com

InfoDefense
Strategic Information Security

Thank you!

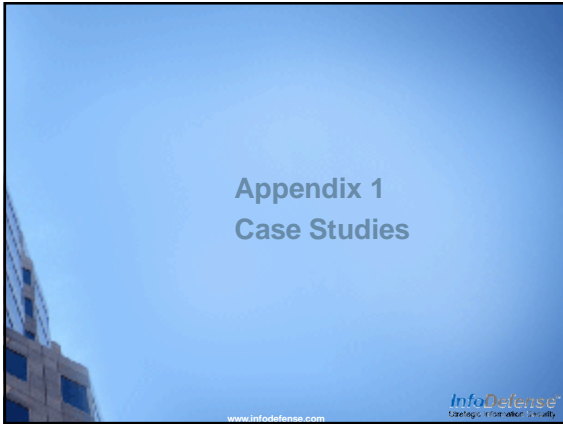
Kevin Wheeler

kevin.wheeler@infodefense.com

Office: (972) 992-3100 Ext. 811

www.infodefense.com

InfoDefense
Strategic Information Security



Heartland Payment Systems

Breach Announced: January 20, 2009
Attack Vector: Malware planted in a server's unallocated disk space that intercepted credit card transactions
Motive: Cyber Crime, Credit Card Fraud
Effect of Breach: Up to 100 Million credit card holder's information was disclosed
Remediation: Removal of the malware, Heartland is also implementing an advanced monitoring and logging system to detect system anomalies in the future

www.infodefense.com

InfoDefense
Strategic Information Security

LA Traffic Control Center

Breach Announced: August 21, 2006
Attack Vector: Stolen Supervisor passwords
Motive: Cyber Terrorism, Union Strike
Effect of Breach: Traffic lights at four key LA intersections were disabled for four days jamming traffic at the intersections
Remediation: Attackers eventually relinquished control of the system. The city most likely changed passwords, implemented more stringent password policies and possibly implemented a strong authentication system.

www.infodefense.com

InfoDefense
Strategic Information Security

US Army Agent.btz Infection

Breach Announced: November, 2008

Attack Vector: Malware entered DoD networks through infected USB drives

Motive: Cyber Espionage

Effect of Breach: Classified

Remediation: USB flash drives and other removable media devices such as floppy disks, CDs, DVDs, cameras, MP3 players and USB hard drives were banned

www.infodefense.com

InfoDefense
Strategic Information Security

Georgia Cyber Attack

Breach Announced: August 11, 2008

Attack Vector: DDoS, SQL Injection and Various other Attack Methods

Motive: Cyber Warfare

Effect of Breach: Georgian government web sites were defaced, Georgian government web sites and Internet Infrastructure were disabled

Remediation: Georgia Moved government web sites to US-based hosting providers, defacements were repaired

www.infodefense.com

InfoDefense
Strategic Information Security

Lessons Learned from Recent Breaches

1. Monitor Network and System Activity Aggressively
2. Control USB flash drives and other removable devices
3. Establish and enforce a sound password policy, Consider implementing two-factor authentication for critical systems
4. Address application vulnerabilities as well as network and platform vulnerabilities
5. Create an incident response plan
6. Encrypt any sensitive data that leaves your offices
7. Protect systems against insider threats
8. Proactively manage system configurations

www.infodefense.com

InfoDefense
Strategic Information Security
