Overview of Information Technology Security

John Christly - NSU CISO
Marlon Clarke - Director IT Security

Presentation Updated 2015-05-14

NSU NOVA SOUTHEASTERN UNIVERSITY
Office of Innovation and Information Technology

Agenda

- PCI Vulnerabilities
- What Makes Us Vulnerable
- What Makes IT Systems Vulnerable
- What Does OiiT do to assist with PCI Compliance
- Breach Examples
- Data Breaches in the News
- What is a Compromise or Security Incident
- How do you report Security Incidents
- Questions

PCI Vulnerabilities

- Vulnerabilities create open doors for theft
- Exist within the credit card ecosystem
- Point of Sale Devices
- Desktops / Laptops
- Servers
- Wireless Hotspots
- Web shopping applications
- Paper based storage systems
- Unsecured transmission of cardholder data

What Makes Us Vulnerable?

- Easily Guessed Passwords.
- Not knowing where sensitive data is.
- Not understanding the risks to the systems that hold PCI data.

What Makes IT Systems Vulnerable?

Easily Guessed Passwords

- Create Hard to Guess Passwords:
- Today's IT systems need to be secured
- Many PCI-related systems are based on computers and have IP Addresses, some have wireless capabilities
- Vendor defaults: having no passwords or default passwords that are known or easily guessed
- Many servers, databases, and applications need generic accounts to run without user intervention

What Makes IT Systems Vulnerable?

Not knowing location of sensitive data

- Inventory of PCI Data Required:
- Systems that hold PCI data should be identified and known to IT / Application support (don't hide them)
- Data flows between systems should be documented
- Use of external storage devices should be reviewed and secured
- Data backup and long term storage should be reviewed and secured (gone are the days where NOT having encryption enabled is an acceptable practice)

What Makes IT Systems Vulnerable?
Not knowing location of sensitive data (cont'd)

- Where do you store your data:
- USB thumb-drives and external hard drives are not the appropriate place to store sensitive NSU data
- Do not take sensitive NSU data with you, by using external storage devices or sending the data to your self via email or using a cloud storage provider
- If you need to send sensitive data via email, contact OiiT to get setup with the ability to encrypt emails (this should be reserved for designated individuals only and should only be used when absolutely necessary)

What Makes IT Systems Vulnerable?

Known Vulnerabilities and Knowledge

- Not understanding the risks to the systems that deal with PCI data.
- Systems to be regularly checked for known vulnerabilities, missing patches, out of date anti-virus, and configuration errors.
- System to manage issues identified so proper response plans can be created, managed, and documented.
- Data being accessed / movements of data to be examined closely: inappropriate access and for data theft.

What Makes IT Systems Vulnerable?

Trusting What We Get from Others

- Internet Access and Downloads
- Be cautious with installing or deleting any software on your work PC.
- Be careful with downloading freeware or shareware from the Internet.
- Wireless Networks
  - Use free wireless in public places with extreme caution.
  - It is very easy for hackers to “sniff” traffic at public hotspots
  - Wireless does not typically come secured “out of the box”, so follow the router/access point directions to secure your home wireless network

What Does OiiT Do to assist with PCI Compliance?

- Responding to regular audits of our Internet-facing technology infrastructure, and we work to fix any identified issues ASAP

- OiiT has developed a new vulnerability management program, which will seek to provide regular scans of our technology infrastructure as well as a focused remediation process.

- Encrypting laptops, desktops, and server hard drives.

- Mobile Device management (MDM) solution to secure devices

Breach Example 1

On a Friday, an employee accepting credit card payment on a kiosk decides to check their email.

Their inbox contains an email from a friend. The subject line reads “Still need tickets?” The message says “He needs to sale these!!! CHEAP!” It contains a link. The employee clicks the link& is taken to a website that has nothing to do with football tickets.

They leave the site, but have already downloaded malware

Breach Example 2

A customer accidentally knocks over her handbag, scattering its contents on the floor behind and under the counter in a checkout line.

While the cashier is distracted helping the customer, a second person switches out the Point of Sale unit with an identical one set up to skim pin numbers and card information.

Thousands of debit and credit card numbers are intercepted before a new POS is installed and the switch is discovered.

Data breaches in the News

- The number of U.S. data breaches tracked in 2014 hit a record high of 783 in 2014 *(Source: Identity Theft Resource Center, 2015*). This represents a substantial hike of 27.5 percent over the number of breaches reported in 2013.

- The number of U.S. data breach incidents tracked also hit a milestone of 5,029 reported data breach incidents, involving more than an estimated 675 million records *(Source: Identity Theft Resource Center, 2015*).

- In the US, data breach incidents cost companies $246 per compromised record in 2013. *(Source: Ponemon Institute, 2014)*

- The average total cost per company that reported a breach in 2013 was $3.5 million. *(Source: Ponemon Institute, 2014)*

Data breaches in the News

- Staples Inc. confirmed last year that about 1.16 million credit cards may have been hit in a major data breach. The culprit was malware that may have allowed access to transaction information including names of cardholders and their card numbers, expiration dates and verification codes, the big retailer said in a statement posted on its website (2014).

- Several financial institutions recently uncovered fraud on credit and debit cards that were recently used at Marriott hotels. The recent breach appears to be linked to hacked point of sale systems at restaurants and bars within the hotels (2014).

Data breaches in the News (cont'd)

- Top Five Breaches in Higher Education *(Privacy Rights Clearinghouse, 2014)*
  - University of Maryland, College Park; 309,079 records
  - North Dakota University; 290,780 records
  - Butler University; 163,000 records
  - Indiana University; 146,000 records
  - Arkansas State University College of Education and Behavioral Science's Department of Childhood Service; 50,000 records

Data breaches in the News

Rank	Sector	Number of Incidents	Percentage of Incidents	100%
1	Healthcare	116	37%	
2	Retail	34	11%	
3	Education	31	10%	
4	Gov. & Public Sector	26	8%	
5	Financial	19	6%	
6	Computer Software	13	4%	
7	Hospitality	12	4%	
8	Insurance	11	4%	
9	Transportation	9	3%	
10	Arts and Media	6	2%	

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

For the fourth year in a row, the healthcare sector reported the largest number of data breaches.

SHARE THIS

Which of the categories in the figure does NSU fall in?

What is a compromise or Security Incident

- Malicious Code – virus, worms, trojan horse, or other malicious code infects a computer

- Inappropriate Usage – an individual violates computing resource policies or the law

- Unauthorized Access – gaining logical or physical access to network, systems, data, application, or other resources without permission

- Theft of data or devices

How do You report Security Incidents

- Contacting Information Security
  - Call the Strategic Support Helpdesk (extension 2-7777)
  - IT Security Hotline (2-0448)
  - Email itsecurity@nova.edu

- IT Security's Role
  - Assess the Situation
  - Determine the extent of incident and loss
  - Collaborate on remediation plan
  - Reporting to insurers and other entities

Additional Resources

We are in the process of adding new policies to the IT policy portal, and we ask that you review them at the link below:
https://www.nova.edu/portal/oiit/policies/

- NSU Enterprise Username and Password Policy
- NSU Organizational Software Policy
- NSU Computer Administrative Rights Policy
- Acceptable Use Policy
- Computer Security Device Standards Policy

Questions?
(We have the time)

- To Contact John Christly
- 954-262-4643
- jchristly@nova.edu

- To Contact Marlon Clarke
- Tel – 954-262-4986
- mrclarke@nova.edu