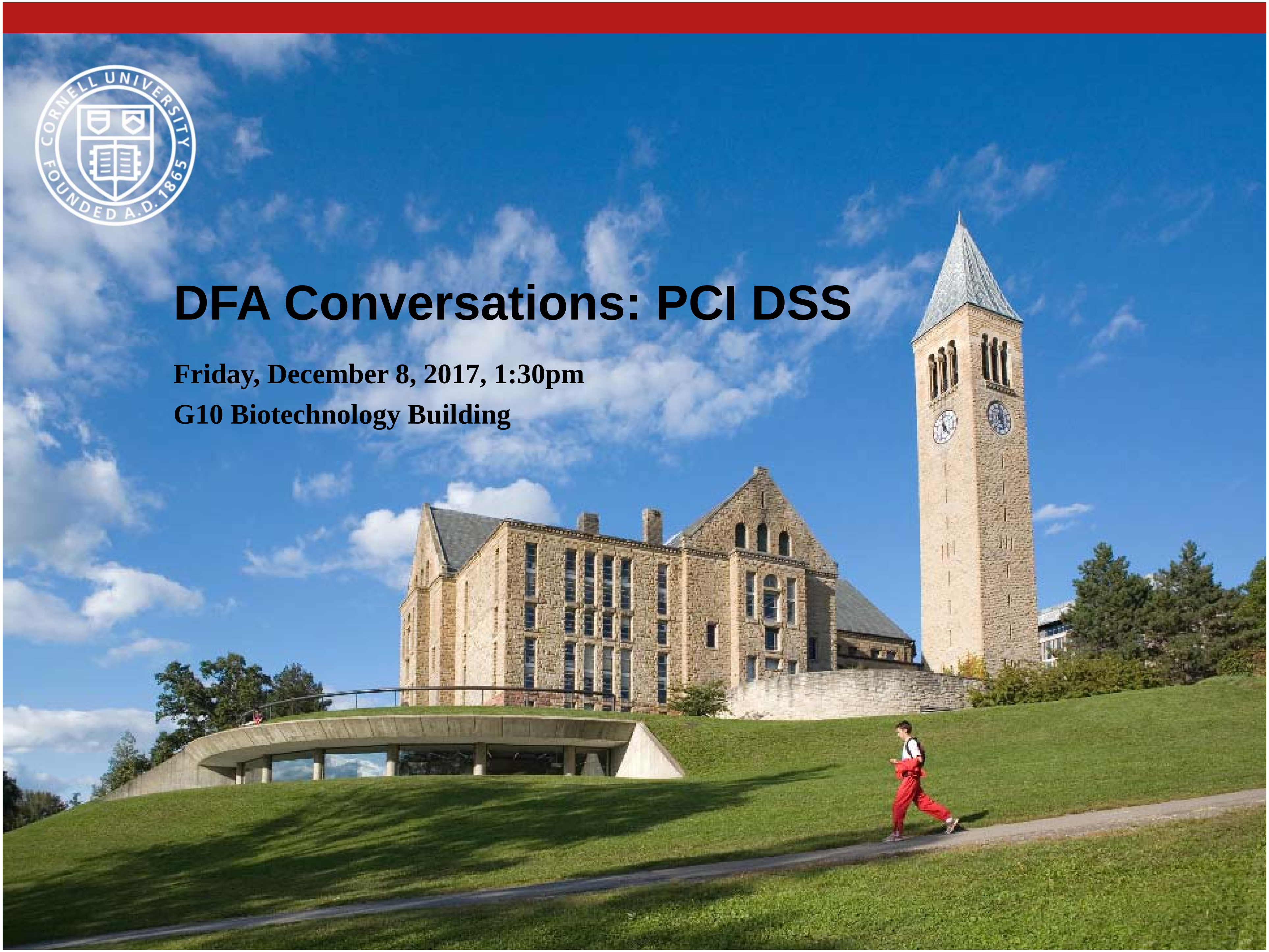


DFA Conversations: PCI DSS

Friday, December 8, 2017, 1:30pm

G10 Biotechnology Building

DFA Conversations: PCI DSS – December 8, 2017

Meeting Agenda

- Introductions
- Cornell’s credit card processing landscape
- Anatomy of a credit card
- What is PCI?
- The PCI DSS
- Safeguarding against fraud
- Credit card breaches
- What to do if a breach is suspected
- What is an SAQ?
- Common PCI compliance problems in higher education
- Questions/Conversation

DFA Conversations: PCI DSS – December 8, 2017

Introductions

Cash Management

Debra Federation

Director of Cash Management

Kevin Mooney

Cash Management Representative

Cornell IT Security Office

Tim Bradish

Assistant Director, Security Operations and Incident Response

Tom Horton

Assistant Director, Identity Management and Security Engineering

Annual Credit Card Income at Cornell*

(Per calendar year)

- CY 2016 – nearly $120 million in net income
- Average growth of about 6% per year since CY 2012
- About 80% of the income is from five departments:
  - Student and Campus Life
  - AA&D
  - Vet School (incl. CUHA)
  - Statler Hotel / SHA
  - School of Continuing Education

***Cash/checks/ACH/wires etc. are NOT included**

DFA Conversations: PCI DSS – December 8, 2017

Cornell Credit Card Processing Landscape

Payment Processors	Payment Channels
FreedomPay	Card-present
Payflow	MOTO
PayPal	eCommerce
Cvent	
Cornell Business Services	

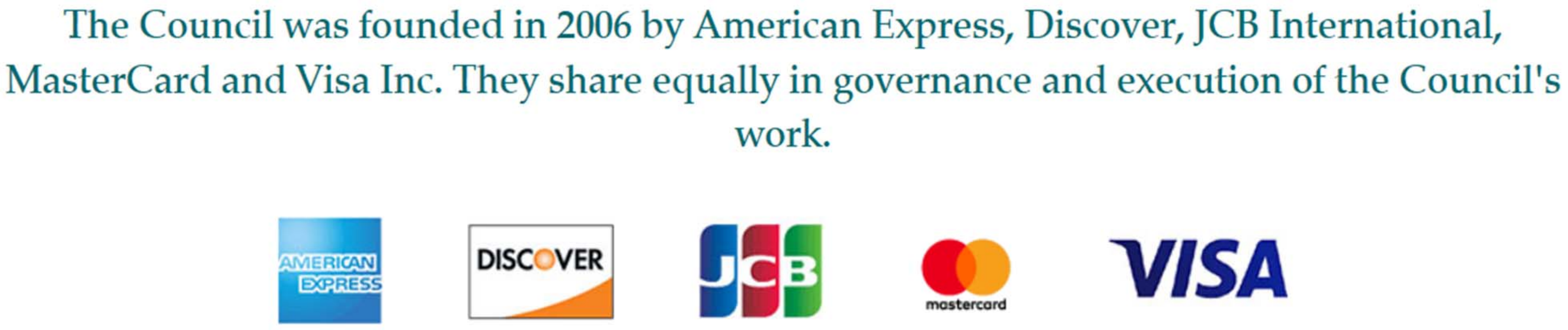
Anatomy of a Credit Card

CREDIT CARD
1234 5678 9876 5432

All digits – Primary Account Number (PAN)
First six digits – Bank Identification Number (BIN)
Next six (or nine) digits – Account number
Last digit – check digit

What is PCI?

Payment Card Industry Security Standards Council

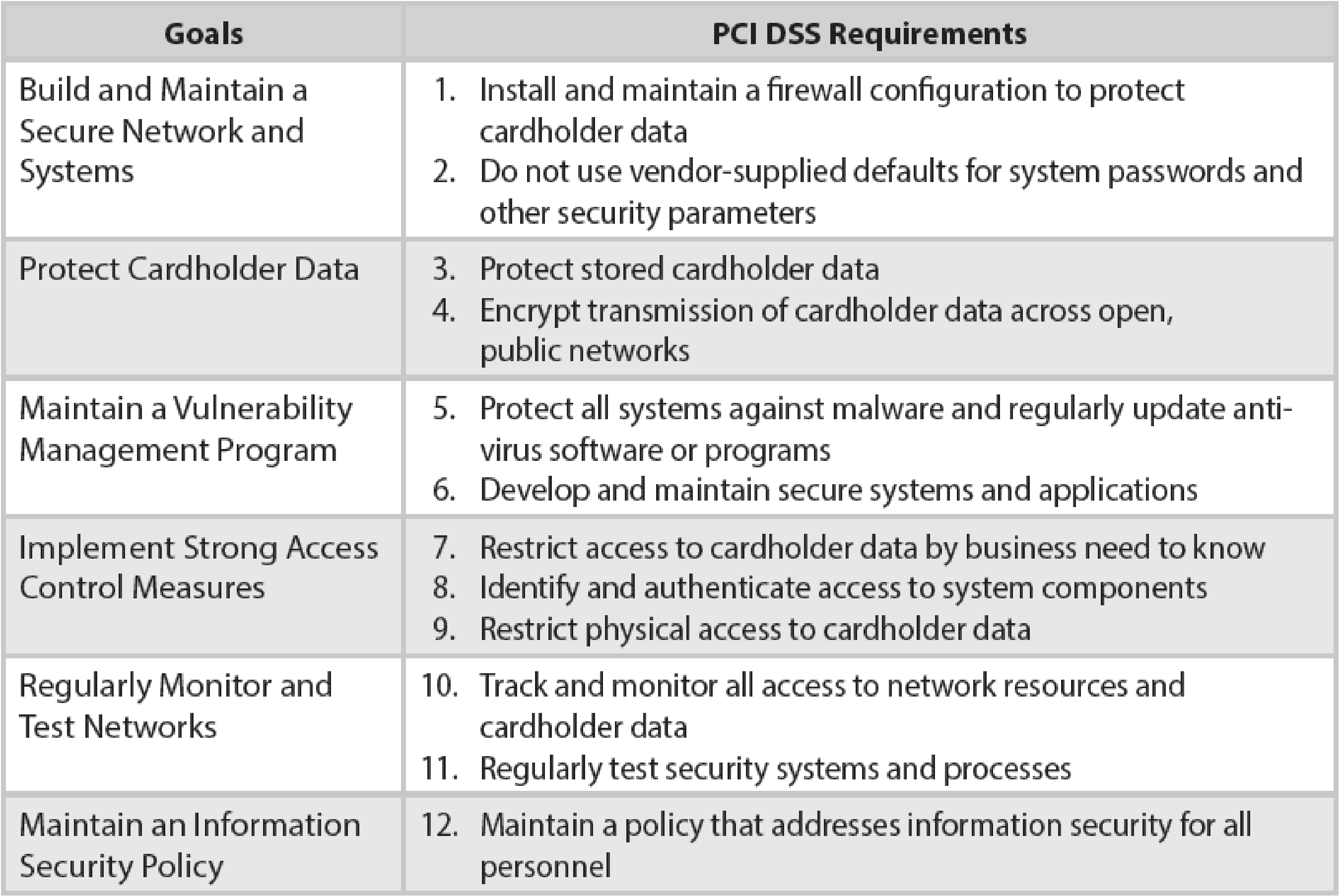


The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work.

Source: https://www.pcisecuritystandards.org/pci_security/

DFA Conversations: PCI DSS – December 8, 2017

The PCI Data Security Standard

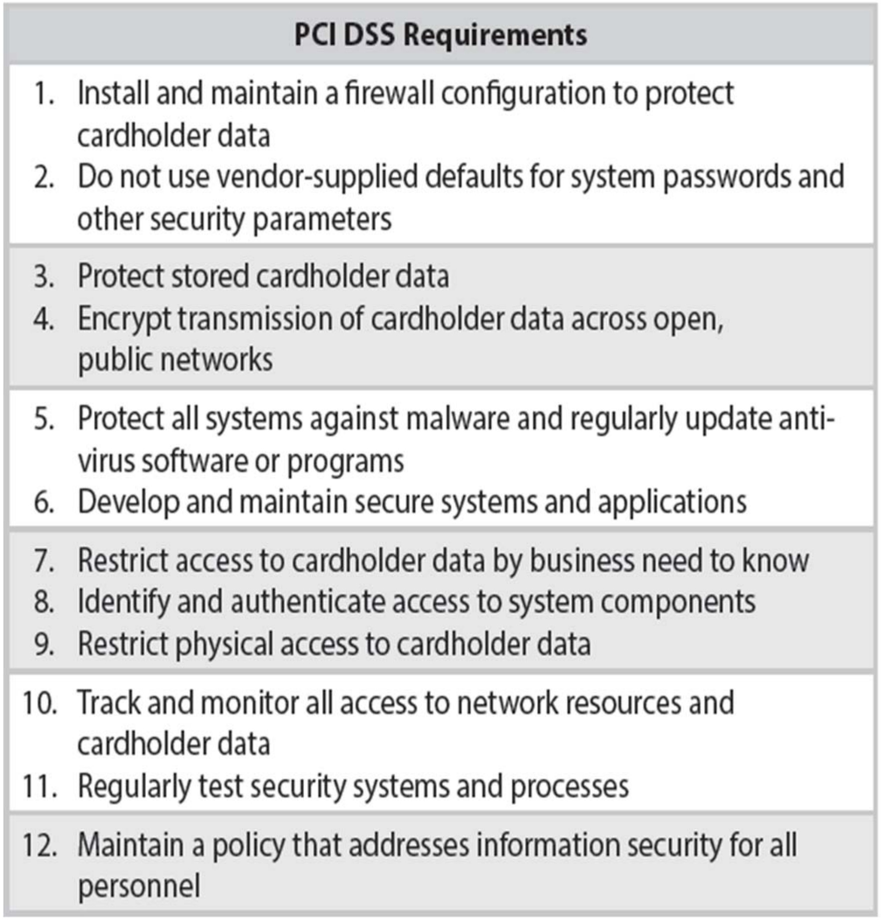


Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

DFA Conversations: PCI DSS – December 8, 2017

What is an SAQ?

- Self-Assessment Questionnaire
  - Attest to compliance with applicable PCI DSS requirements
- Different SAQ types depending on how transactions are processed
  - Third-party eCommerce (Payflow, Cvent) = SAQ A (22 questions)
  - P2PE Devices (FreedomPay) = SAQ P2PE (33 questions)
  - Use of POS w/ Internet connection = SAQ C (162 questions)
  - All others – SAQ D (331 questions)
- Roughly 87% of Cornell's 49 SAQs were either P2PE or A



PCI DSS Requirements
1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

The PCI Data Security Standard

Requirement 2:

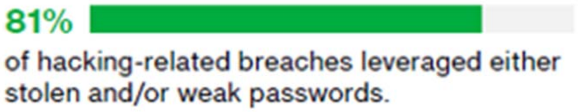
Do not use vendor-supplied defaults for system passwords and other security parameters

- Change vendor-supplied defaults BEFORE installing a system on the network
- Remove/disable unnecessary default accounts BEFORE installing a system on the network

Requirement 8:

Identify and authenticate access to system components

- Do users have a unique ID before allowing access to system components or cardholder data?
- Is access for terminated users immediately deactivated or removed?



of hacking-related breaches leveraged either stolen and/or weak passwords.

Source: Verizon 2017 Data Breach Investigations Report

DFA Conversations: PCI DSS – December 8, 2017

The PCI Data Security Standard

Requirement 3:

Protect stored cardholder data

- Delete CHD (cardholder data) when no longer needed
- Retention policy?
- Is data checked against this policy?

DFA Conversations: PCI DSS – December 8, 2017

The PCI Data Security Standard

Requirement 9:

Restrict physical access to cardholder data

- Are all media physically secured?
- Are hardcopy materials crosscut-shredded?
- Is a list of devices maintained and updated when needed?
- Are devices periodically inspected to detect tampering or substitution?

DFA Conversations: PCI DSS – December 8, 2017

Safeguarding Against Fraud

Raw Video: Men Place Card Skimmer on ATM Store Machine!

YouTube Link: https://youtu.be/y83ZgzuFBSE

DFA Conversations: PCI DSS – December 8, 2017

Safeguarding Against Fraud

How to spot credit card skimmers before it's too late

YouTube Link: https://youtu.be/C7Rfup4vIVQ

The PCI Data Security Standard

Requirement 12:

Maintain a policy that addresses information security for all personnel

- Is a security policy established, published, maintained, and distributed to all relevant personnel?
- Do security policy and procedures clearly define information security responsibilities for all personnel?
- Has an incident response plan been created to be implemented in the event of a system breach?

Credit Card Breaches

- Heartland Payment Systems: 130 million cards
- TJX Companies: 94 million cards
- TRW/Sears: 90 million cards
- Home Depot: 56 million cards
- Target: 40 million cards

Source: https://www.investopedia.com/news/5-biggest-credit-card-data-hacks-history/

DFA Conversations: PCI DSS – December 8, 2017

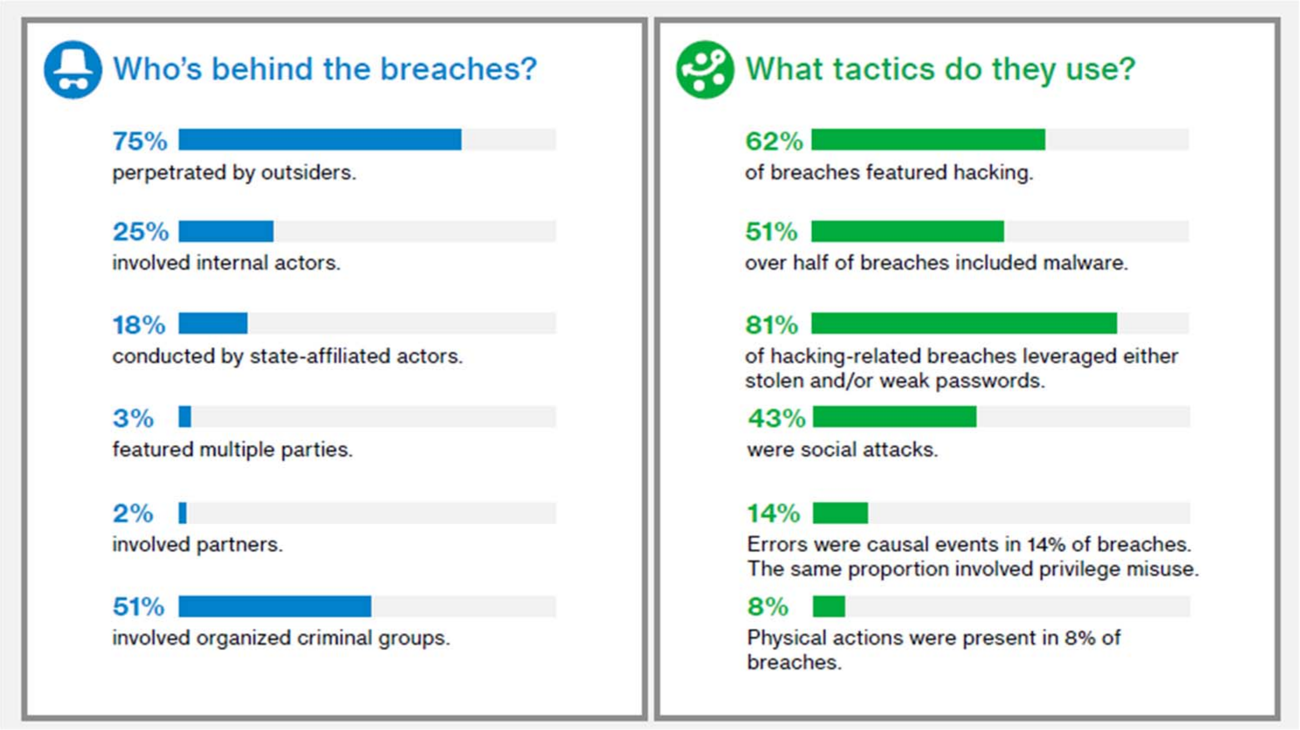
Detecting Breaches

Point of sale / back-end system / eCommerce

- Anomalous / fraudulent charges reported by clients
- Unusual system behavior
- Skimmer found on POI hardware
- External report from Bank/Law Enforcement

© Randy Glasbergen.
www.glasbergen.com
GLASBERGEN
"IT LOOKS LIKE EVERYONE WILL BE GETTING WHAT THEY WANT THIS YEAR...SOMEBODY POSTED MY CREDIT CARD NUMBER ON THE INTERNET!"

Background on Breaches



Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Source: Verizon 2017 Data Breach Investigations Report | http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

DFA Conversations: PCI DSS – December 8, 2017

What to Do If a Breach Is Suspected

- Notify support functions
- Local IT Support / IT Security / Cash Management
- Suspend credit card processing
- Initiate Incident Response process with IT Security Office

Common PCI Compliance Problems in Higher Education

- Payment card information is processed on computers also used for Internet access
- Staff are processing credit card numbers received via unencrypted email
- Policies and procedures regarding the handling of payment card data are incomplete or nonexistent
- A formal security awareness training does not exist or is not provided consistently on an annual basis
- Improper oversight of third party vendors that handle payment card data
- Passwords are written down and/or shared

Source: CampusGuard News

Employee PCI Training

- Who should take it?
  - Any employee who handles cardholder data, and anyone who supervises those employees
- When?
  - Immediately upon hire and every year thereafter
- Where?
  - CU Learn; search for ‘PCI Annual Awareness Education’

DFA Conversations: PCI DSS – December 8, 2017

Additional Resources

Cornell University Policy 3.17 – Accepting Credit Cards to Conduct University Business:

https://www.dfa.cornell.edu/sites/default/files/policy/vol3_17.pdf

PCI Security Standards Council:

https://www.pcisecuritystandards.org

PCI DSS Quick Reference Guide:

https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf

Verizon 2017 Data Breach Investigations Report:

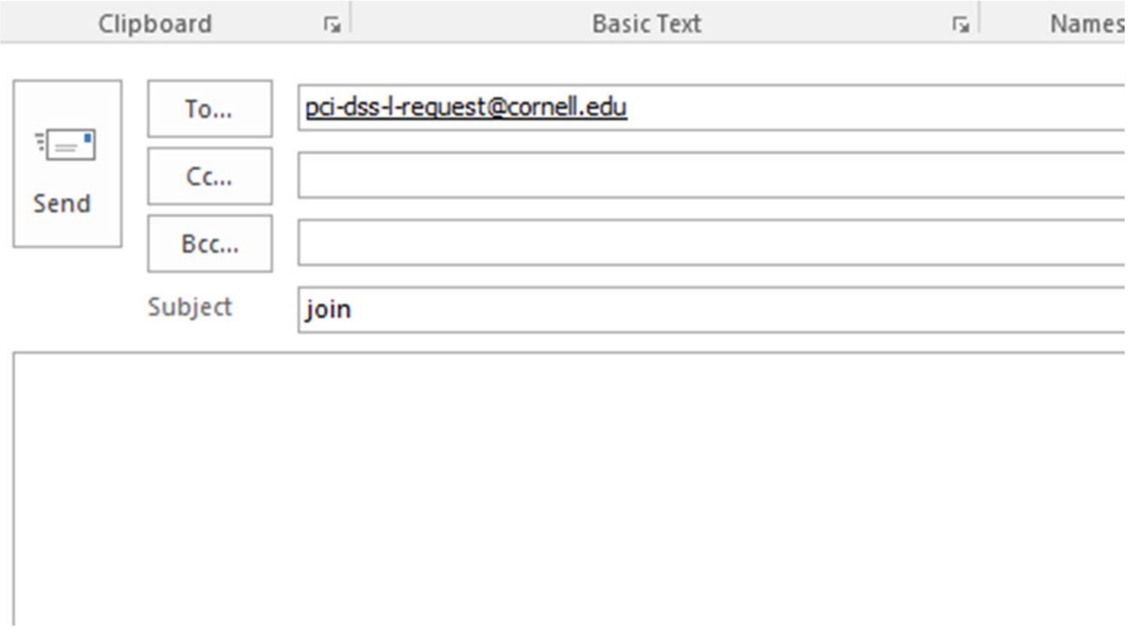
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

DFA Conversations: PCI DSS – December 8, 2017

Questions?

pci-help@cornell.edu

To join the PCI-DSS-L listserv:



To... pci-dss-l-request@cornell.edu

Subject join

https://it.cornell.edu/lyris/join-e-lists-lyris

Thank you!