Strengthening Processor Security Webinar

10:00 AM – 11:00 AM PT

October 16, 2013

Strengthening Processor Security Webinar

Welcome and Overview

Mamie Lee
Business Leader
Visa Third Party Risk

Strengthening Processor Security Webinar

Agenda

10:00 AM – 10:05 AM	**Welcome** Mamie Lee, VisaNet Processor Risk
10:05 AM – 10:15 AM	**Strengthening Processor Security – Going Beyond** Oscar Munoz, Visa Third Party Risk
10:15 AM – 10:25 AM	**Visa's View on Cyber and Enterprise Security** Dale Compton, Visa Global Information Security
10:25 AM – 10:45 AM	**New Challenges Facing Processors** Joseph Pierini, PSC*
10:45 AM – 11:00 AM	**Question and Answer**

*For a list of Qualified Security Assessor (QSA) companies, refer to the PCI Security Standards Council website at https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php. Visa is not endorsing the services of any specific QSA and is not guaranteeing any kind of immunity from enforcement of Visa policies.

Strengthening Processor Security – Going Beyond

Oscar Munoz
Business Leader
Visa Third Party Risk

Forward Looking Statement Disclaimer

This presentation contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms including but not limited to the following: “believe,” “continue,” “could,” “estimate,” “expect,” “intend,” “may,” “potential,” “should,” “will,” and similar references to the future. Examples of such forward-looking statements include, but are not limited to statements about expected efficacy of Risk strategies and fraud trends.

By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following:

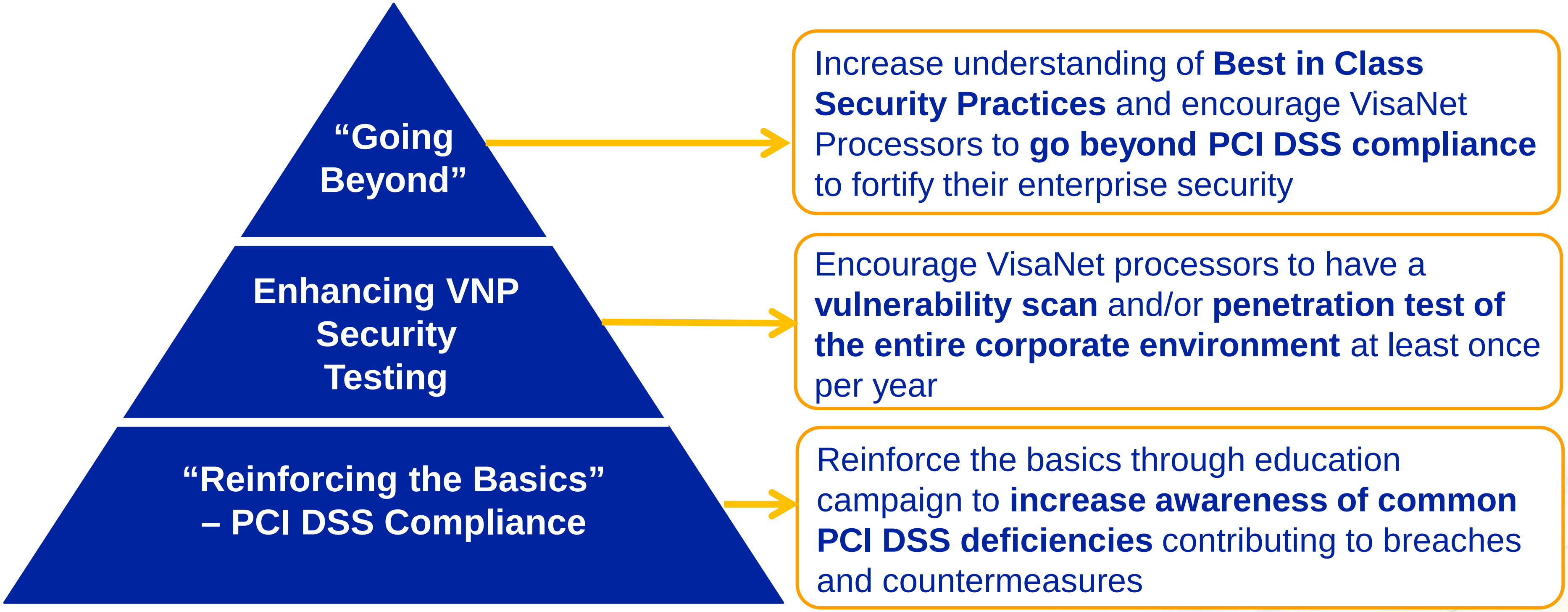
- The impact of laws, regulations and marketplace barriers, including:
  - increased regulation outside the United States and in other product categories;
  - fraud trends and technological evolutions; and
  - rules about consumer privacy and data use and security;
- developments in litigation and government enforcement;
- economic factors, such as:
  - global economic, political and health conditions;
  - cross-border activity; and
- industry developments, such as competitive pressure and rapid technological developments;
- system developments, such as:
  - disruption of our transaction processing systems or the inability to process transactions efficiently;
  - account data breaches or increased fraudulent or other illegal activities involving our cards; and
  - issues arising at Visa Europe, including failure to maintain interoperability between our systems;
- loss of organizational effectiveness or key employees;
- failure to integrate acquisitions successfully or to effectively develop new products and businesses;
- and the other factors discussed under the heading "Risk Factors" in our most recent Annual Report on Form 10-K on file with the U.S. Securities and Exchange Commission. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement because of new information or future developments or otherwise.

Disclaimer

The information, recommendations or “best practices” contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations, programs or “best practices” may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Strengthening Processor Security

Visa is launching a campaign to reinforce security basics and encourage going beyond the PCI DSS



"Going Beyond"

Increase understanding of **Best in Class Security Practices** and encourage VisaNet Processors to **go beyond PCI DSS compliance** to fortify their enterprise security

Enhancing VNP Security Testing

Encourage VisaNet processors to have a **vulnerability scan** and/or **penetration test of the entire corporate environment** at least once per year

"Reinforcing the Basics" – PCI DSS Compliance

Reinforce the basics through education campaign to **increase awareness of common PCI DSS deficiencies** contributing to breaches and countermeasures

Strengthening Processor Security

The PCI Data Security Standard (PCI DSS) is an on-going obligation. Specific requirements can be found at https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0.

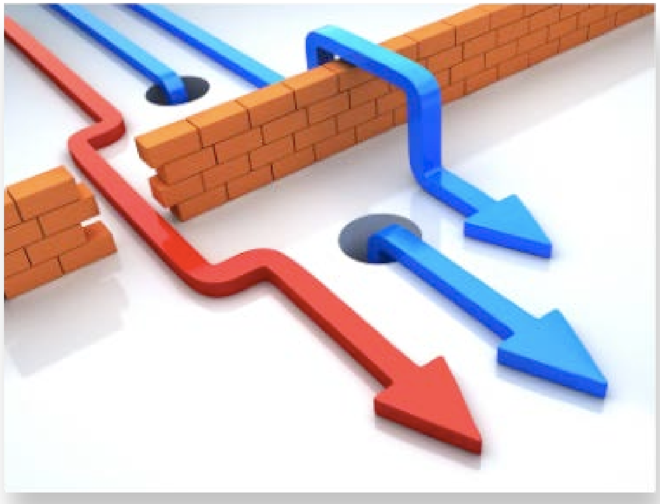
Reinforcing the Basics

1. Increase segmentation security between corporate network and cardholder data environment
2. Maintain a robust inventory of cardholder data (CHD). Know where CHD is, when it changes or is transferred and all systems that are connected to CHD systems
3. Maintain a robust incident detection and response process
4. Ensure the use of vulnerability management and secure coding
5. Install web application firewalls to combat SQL injection attacks
6. Harden databases by improving security controls and operating systems by minimizing security vulnerabilities

Strengthening Processor Security

PCI DSS requires quarterly vulnerability scans and an annual penetration test of the cardholder data environment.

Visa recommends enhancing the scope of the scans and tests to include the entire corporate environment. Visa encourages processors to share that they are performing the enhanced testing with their sponsors.



Enhancing VNP Security Testing

Perform quarterly **vulnerability scan** and/or **penetration test** of the entire **corporate environment** at least once per year

- Visa to advise QSAs to note in ROC when an entity has performed these scans or penetration tests
- Visa will also encourage VisaNet processors to share this information with their banks sponsors
- Bank sponsors will be urged to ask their VisaNet processors about scans and tests performed that go beyond the PCI DSS

Strengthening Processor Security

Going Beyond to Implement Best in Class Security Practices

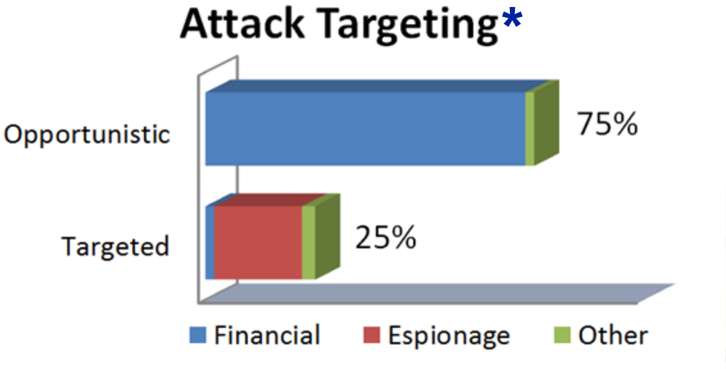
1. Maintain robust enterprise security plan
2. Bolster use of internal audit to ensure continuous compliance
3. Establish a direct line to executive management for info security function
4. Use application penetration tests and vulnerability scans anytime there is a change to the environment
5. Apply PA-DSS to all internally-developed software
6. Deploy tools such as: Security Information and Event Management (SIEM) and Data Loss Prevention (DLP)
7. Use IP/Internet traffic monitoring
8. Use application white listing to identify and allow known “good files”
9. Periodically rotate primary QSA assessor or QSA company

Visa's View on Cyber and Enterprise Security

Dale Compton
Business Leader
Visa Global Information Security

Cyber Security – a National Imperative

- An Executive Order dated February 2013 stressed that cyber threats to critical infrastructure are increasing and “represents one of the most serious national security challenges” faced by the U.S. Government.
- In March 2013, Director of National Intelligence, James Clapper, published a report stating that cyber threats (cyber attacks & cyber espionage) are the #1 threat ahead of terrorism, transnational organized crime, and WMD.
- The electronic payments industry faces cyber threats on a global scale with Visa’s brand being a prime target for cyber threat actors.



*Verizon Data Breach Investigation Report 2013

Visa's View of Enterprise Security

Security Decision Constraints

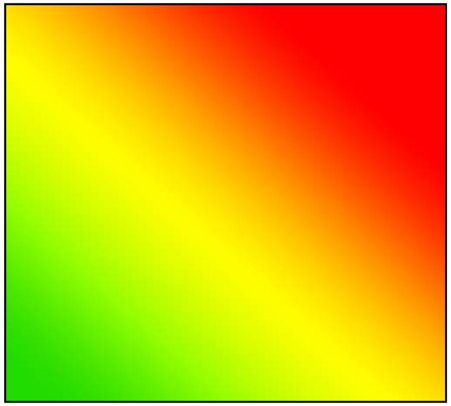
- View security through the lens of **competition**

- Employ **risk and maturity** as competitive levers

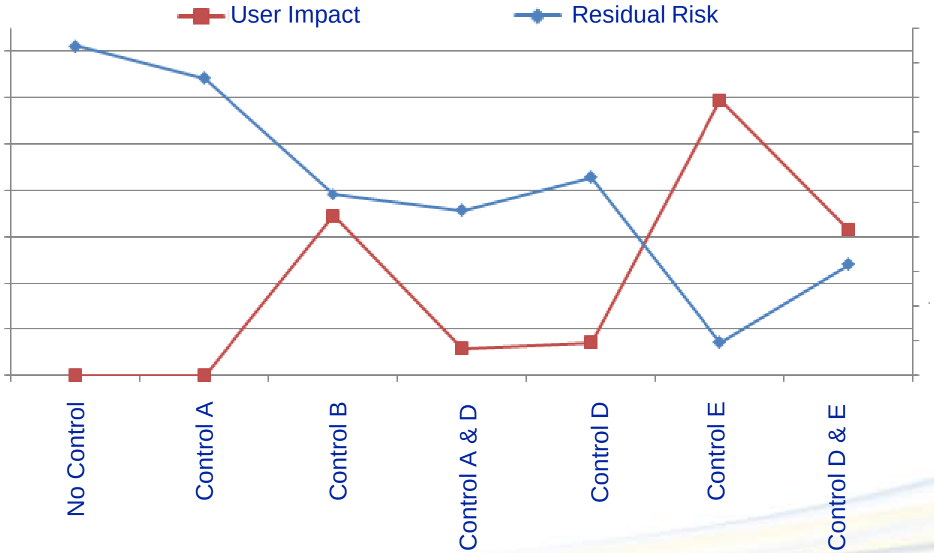
- Drive strategic alignment with **security capabilities**

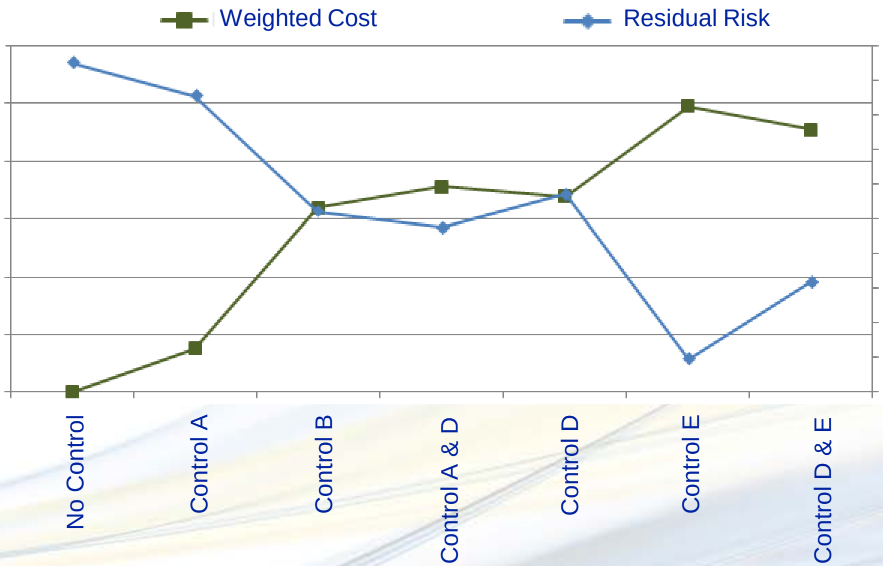
Control Investment Methodology

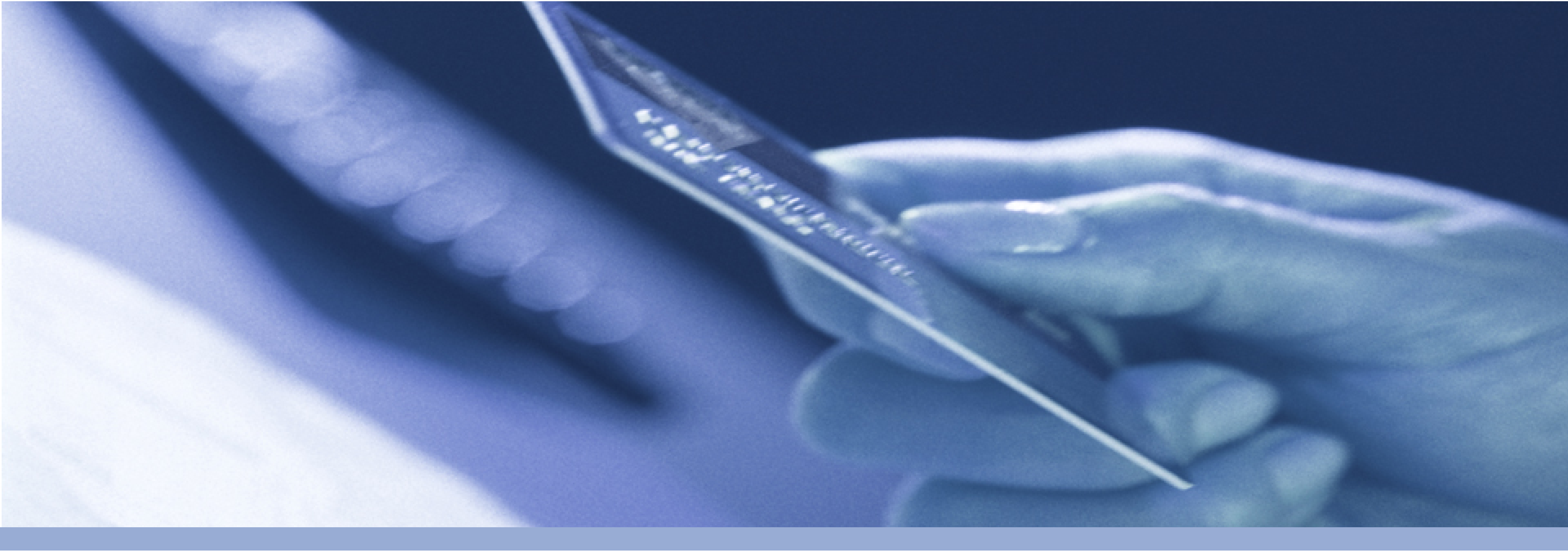
Considering Risk Reduction, User Experience, and Total Cost



Residual Risk **User Impact** **Total Cost**







New Challenges Facing Processors

Attacks and issues that are over and above PCI

PSC

PAYMENTS : SECURITY : COMPLIANCE

Payment : Security : Compliance

- Operations in the USA, UK, Canada and Australia
- Global PCI, PA-DSS, P2PE Assessor and Approved Scanning Vendor.
- One of a select few companies qualified worldwide to provide expert services and solutions to organizations that require specialist compliance or consulting support in the areas of Payments, Security or Compliance.
- Our focus is exclusively on Clients that accept or process payments or technology companies in the payment industry.
- Our Security Lab specializes in internal penetration testing, social engineering, web application testing, malware analysis and external penetration testing.

Intro Slide

- **Joseph Pierini**
  - CISSP, PCI:QSA, PA-QSA, QAE
  - Director of Technical Services
  - Over 15 years in administration and security
  - Active penetration tester performing internal, external, wireless and social engineering engagements.
  - Published vulnerability researcher:
    - Apache Tomcat, Caucho's Resin Application Server, Search Engines, Web Application Firewalls and various Ecommerce Shopping Carts.

Remember:

It's not out of scope if it can be used against you.

Definition of the PCI Data Security Standard 3.0, Requirement 11.3

- 11.3 Develop and implement a methodology for penetration testing that:
  - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).
  - Includes coverage for the entire CDE perimeter and critical systems.
  - Includes testing from both inside the network, and from outside of the network attempting to get in.
  - Includes testing to validate any segmentation and scope-reduction controls.
  - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5.
  - Defines network-layer penetration tests to include components that support network functions as well as operating systems.
  - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months.

Even with the Standard, Breaches Still Occur

- Compromises are expensive: Up to $199 per record.
  - 2013 Cost of Data Breach Study - Symantec
- 70% of attacks aren't detected until 3-12 months after .
  - Verizon Breach Report 2013
- Financial Institutions and Restaurants are still #1 .
  - Verizon Breach Report 2013
- Outsiders are still the #1 threat, insiders make up only 14-25% of reported compromises.
  - Verizon Breach Report 2013
- Hackers are using a 1-2 punch of malware and vulnerability vectors.
  - Trustwave Global Security Report - 2013

Bob in accounting is the new target.

- The majority of compromises result from indirect attacks against the Cardholder Data Environments.

- Hackers are gaining a foothold elsewhere first - typically your corporate network.

- Expand your scope to reduce your risk.

Meet the new threat landscape

- You can't secure the entire corporate network - too many moving parts.
- Hackers may be in the corporate network for weeks or months.
- They will find the path into the CDE if one exists.

Fact:

The level of effort expended is equal to the value of the target.

Pen Test Notes From The Field

- It only takes one password.
  - Man in the Middle Attacks are still really effective.
  - Password reuse is frequent.
  - Password cracking tools are becoming incredibly efficient.

Pen Test Notes From The Field

- It only takes one system.
  - It’s much easier to hack a workstation than a server.
  - Common local administrator passwords create a domino effect.
  - There are new tools for looting systems.

Pen Test Notes From The Field

- If Antivirus doesn't work, why do you still want me to install it?
  - Antivirus is still your first line of defense.
  - Triangulate AV alerts with other monitoring systems.
  - Consider different vendors for different environments.

Rule of Thumb:

Absence of evidence is not evidence of absence.

-- Carl Sagan, Astronomer

Reduce the Corporate Threat

- Identify and Isolate Privileged Users
  - “People” are part of the CDE.
  - If they touch card data or manage systems that do, their systems and credentials need to be protected a securely as the data itself.
  - You can’t hack what you can’t see or what you don't know about.

Reduce the Corporate Threat

- Don't share authentication mechanisms between environments.
  - The CDE needs to have a separate and distinct authentication system.
  - Do not share accounts across authentication systems.
  - Remind users not to use the same passwords across authentication systems.

Reduce the Corporate Threat

- Employ 2-factor authentication and remote access systems to access the CDE.
  - Use remote access protocols with strong logging and account lock-out mechanisms.
  - Implement strong ingress controls.
  - Avoid using soft tokens.

So What Do I Do First Thing Tomorrow?

- Identify and isolate your privileged users.
  - Make sure their systems have unique passwords and personal firewalls.
- Review your password creation policies.
  - Remind your users of your corporate standards.
- Review your monitoring and alerting systems.
  - Test that your antivirus and malware are sending proper alerts.
- Review your CDE access rules.
  - Ensure that CDE access uses 2-factor authentication and there are no direct connections to the CDE.

In Summary:

Confidence is ignorance. If you're feeling cocky, it's because there's something you don't know.

-- Eoin Colfer.

Q & A