



# Information Security Management Training

PAM EVERITT

NIOTEC SOLUTIONS

JULY 20, 2017

# Training Considerations


- ▶ Common Threats
- ▶ Complexity
- ▶ Responsibility and accountability
- ▶ Training for IT personnel and operations management

# Verizon 2017 Data Breach Investigations Report: 10<sup>th</sup> Edition

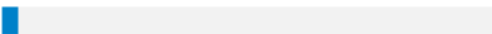


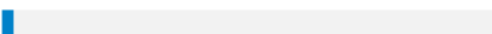
## Who's behind the breaches?


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.

# Verizon 2017 Data Breach Investigations Report: 10<sup>th</sup> Edition



## 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.

# Verizon 2017 Data Breach Investigations Report: 10<sup>th</sup> Edition



## What else is common?

**66%** of malware was installed via malicious email attachments.

**73%** of breaches were financially motivated.

**21%** of breaches were related to espionage.

**27%** of breaches were discovered by third parties.

# The Complexity: laws and regulations

GLBA  
FPA  
COPPA CALEA  
PIPEDA GISRA  
CFAA  
CCCA FISMA  
FERPA CSA<sup>ECPA</sup> OECD  
HIPAA  
HITECH



Who is responsible for Information Security?

**EVERYONE**



Who is ultimately accountable?

# Executive Management

# USCG Cyber Security Guidelines for FSP related to cybersecurity

- ▶ Apply NIST Cybersecurity Framework
- ▶ Apply NIST Special Publication 800-82:  
Guide to Industrial Control Systems (ICS) Security
- ▶ Assess vulnerabilities
- ▶ Ensure facility security:  
“The FSO is required to ensure that facility security persons possess necessary training to maintain the overall security of the facility.”

# Security Training for IT and Management

- ▶ CISSP: Certified Information Systems Security Professional: high-level credential focused on security policy and mgmt. (ISC)2 (International Information Systems Security Certification Consortium) is a nonprofit membership association for credentialing with membership over 125,000.
- ▶ CISA: Certified Information Systems Auditor: designed for professionals who audit, control, monitor and assess information technology and business systems.
- ▶ CISM: Certified Information Security Manager: geared towards people in managerial position; administered by ISACA, an international professional association focused on IT governance which began in 1967.
- ▶ GSEC: GIAC Security Essentials: demonstrates skills in IT systems roles with respect to security tasks. GIAC (Global Information Assurance Certification) is the leading provider and developer of cyber security certifications particularly for government and military organizations.
- ▶ Security+: for systems administrators administered by Comp TIA, the leading provider of vendor-neutral IT certifications.

# Thank you

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted; none of these measures address the weakest link in the security chain.”

– Kevin Mitnick, “The World’s Most Famous Hacker”

Pam Everitt  
Pam.Everitt@Niotec.com  
Office: 843-779-0392  
Cell: 843-514-3955