Texas Society of CPA Certified Public Accountants

2017 Annual Meeting of Members and Board of Directors Meeting

Dan Domagala; *"Cybersecurity: An 8-Point Checklist for Protecting Your Assets"*

Join this interactive discussion about cybersecurity trends, how to identify and assess risk, and taking preventative measures to defend sensitive information. We'll take a proactive approach to reducing vulnerabilities by outlining some sensible actions to help protect you and your clients.

EKS&H
AUDIT | TAX | CONSULTING

AGENDA

- Cybersecurity challenges today
- Security questions… and answers
- Preventative approach with 8-point security inspection

EKS&H AT A GLANCE

WHAT EKS&H IS DOING IN CYBERSECURITY

- Commitment and Investment
  - Cybersecurity Vulnerability Assessment
  - Risk Advisory Services
  - Awareness Training

- Technology Partners
  - Managed Security Service Providers
  - Breach Response and Forensics

AUDIENCE PARTICIPATION

- What cybersecurity topic is top-of-mind for you?

LATEST SECURITY HEADLINES

AIRWAY OXYGEN INC.
HOME MEDICAL EQUIPMENT

Data Breach

Ransomware Attack Affects 500,000 Patients

Marianne Kolbasuk McGee • June 26, 2017

A ransomware attack on a provider of oxygen therapy has resulted in the second largest health data breach posted on the HHS tally so

Authentication

British Parliament Targeted by Brute-Force Email Hackers

Mathew J. Schwartz • June 26, 2017

Members of Parliament in Britain have had their remote email access suspended following an apparent brute-force hack attempt

gain access to their

ail accounts appear to have

Anthem. BlueCross BlueShield

Breach Response

$115 Million Settlement in Massive Anthem Breach Case

Marianne Kolbasuk McGee • June 23, 2017

Health insurer Anthem has agreed to a proposed $115 million deal to settle a class action lawsuit over a 2015 cyberattack that resulted

Anti-Malware

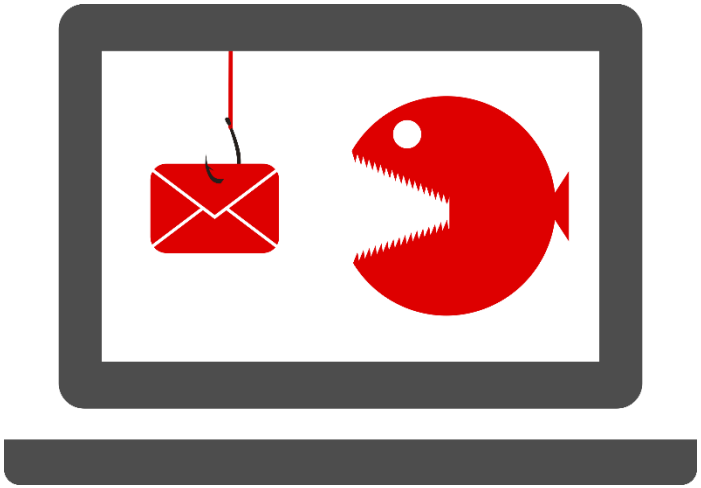
Honda Hit by WannaCry

Mathew J. Schwartz • June 21, 2017

One month after the SMB-targeting WannaCry worm outbreak began spreading globally, Honda discovered fresh infections at multiple facilities, and was forced to temporarily idle one plant as a

CURRENT TRENDS

- Business Email Compromise / Spearphishing
  - Increased 270% since 2015, Average loss of $140,000 (TrendMicro)



- Ransomware
  - up 172% in 2016
- Credential Stuffing
  - Using usernames/passwords from one account to hack another

CYBER SECURITY QUESTIONS AND ACTIONS

1. How secure is my enterprise?
2. What information do I have?
3. Rules and regulations?
4. Who has access?
5. How is access enforced?
6. Identifying suspicious activity?
7. What is my response plan?
8. How susceptible are my employees?

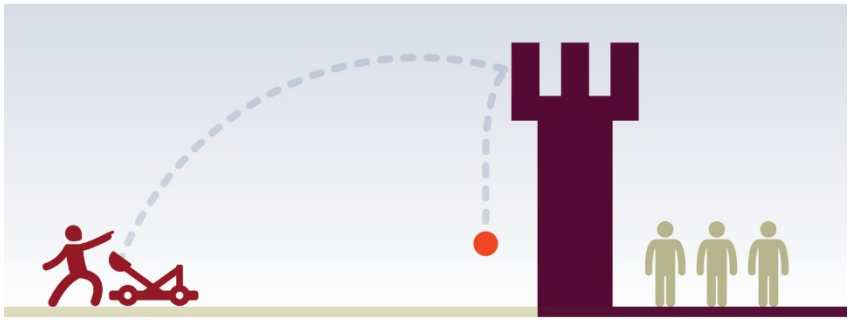
QUESTION #1

How secure is my enterprise?

ACTION: PERIMETER DEFENSE

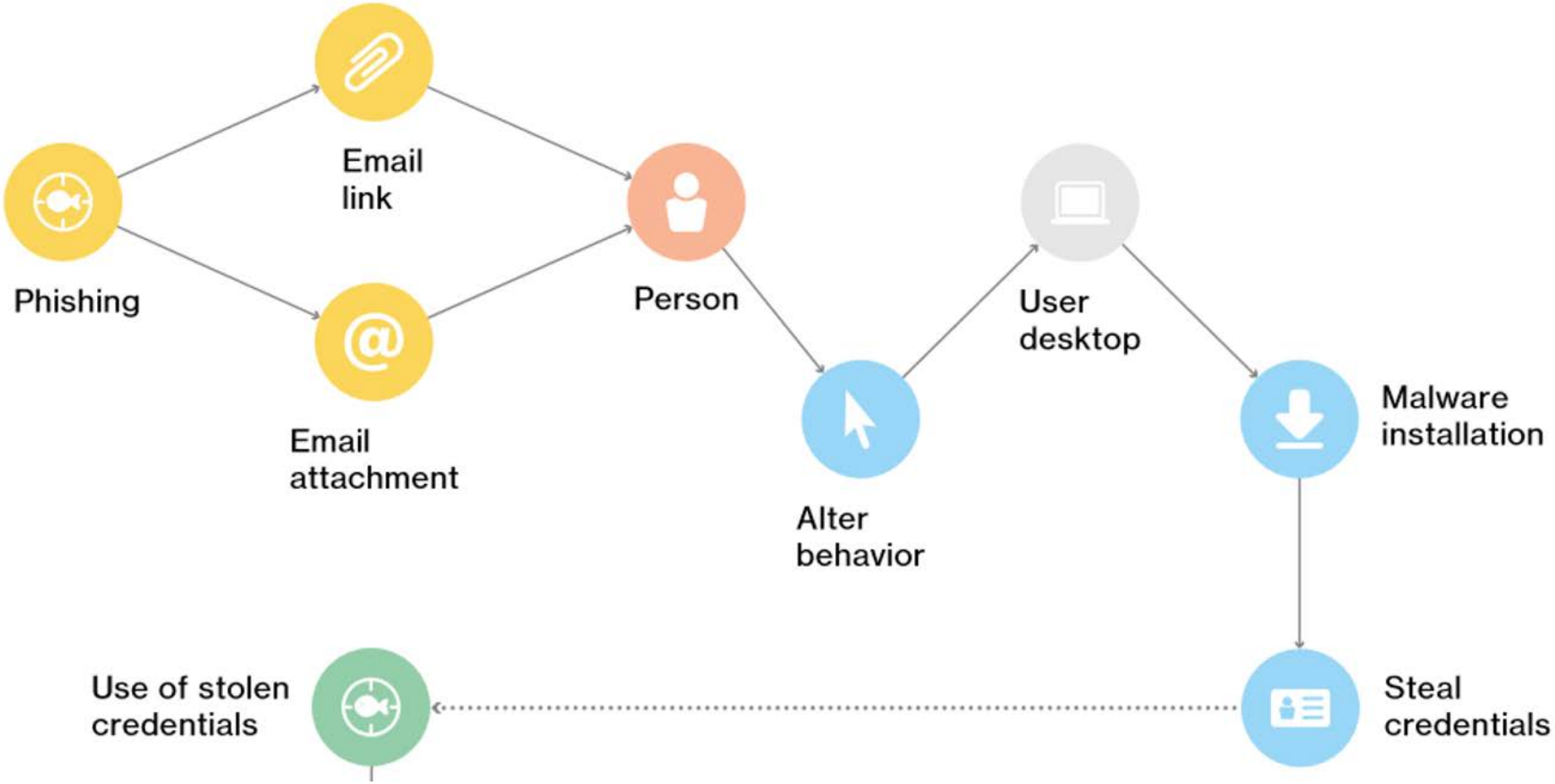
- Defend your castle:
  - Endpoint security
  - Network segmentation
  - Firewall
  - Anti-malware
  - Secure communications

Don't allow yourself to be an easy target.



Defend your perimeter.

ANATOMY OF A BREACH



Source: Verizon 2016 Data Breach Investigations Report

ACTION: PERIMETER DEFENSE

- An ounce of prevention is worth a pound of cure:
  - External vulnerability scanning
  - Internal vulnerability scanning
  - Web/content filtering
  - Email filtering
  - Implement security best practices
  - Trust but verify
- Take the extra step:
  - Two-factor authentication
  - Targeted threat protection

QUESTION #2

What information
do I have?

ACTION: DATA INVENTORY

- Every organization has sensitive information that resides in many places.

WHAT IS THE MOTIVE?

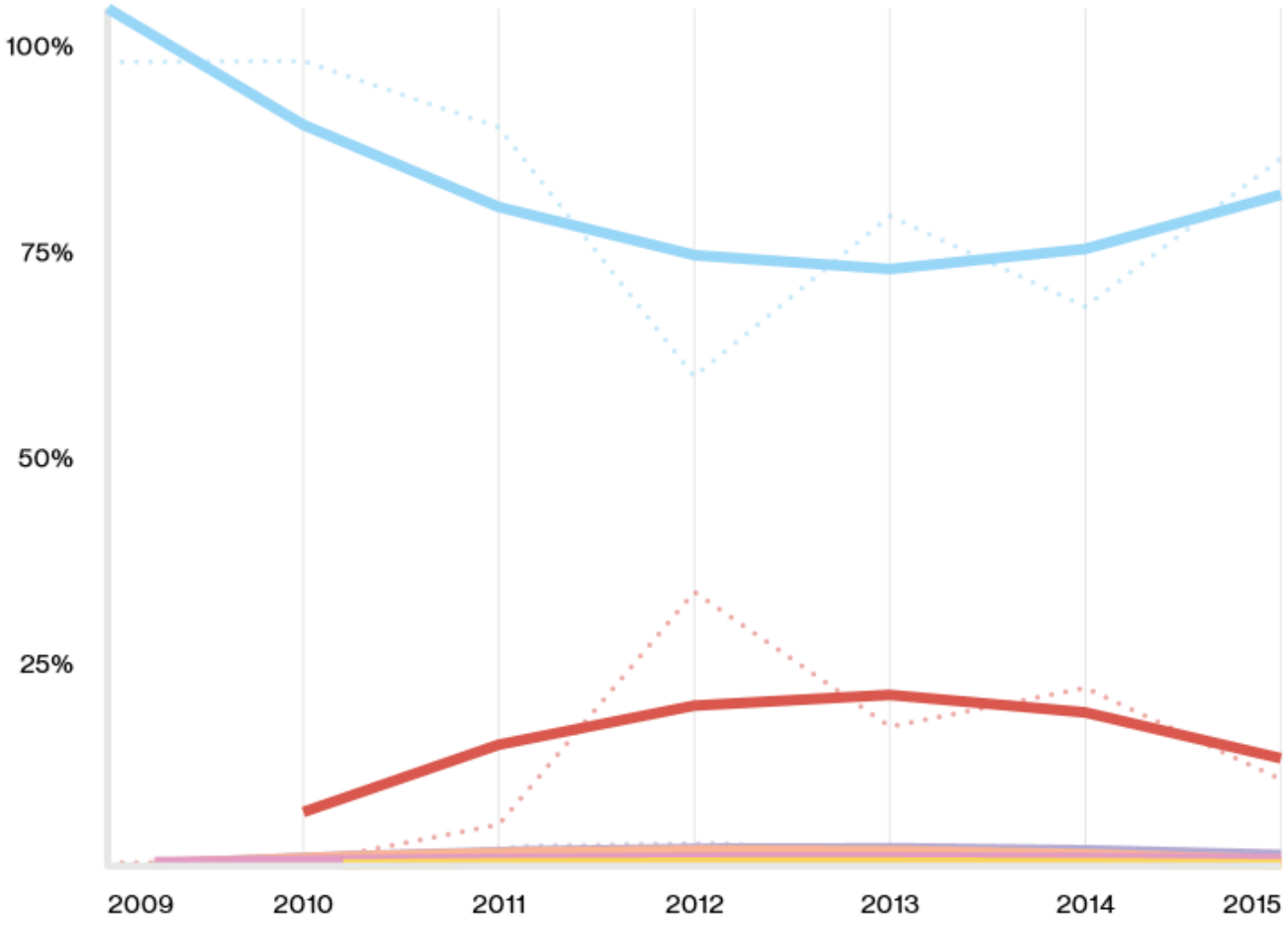


Figure 3.

Percent of breaches per threat actor motive over time, (n=6,762)

Verizon 2016 Data Breach Investigations Report

ACTION: DATA INVENTORY

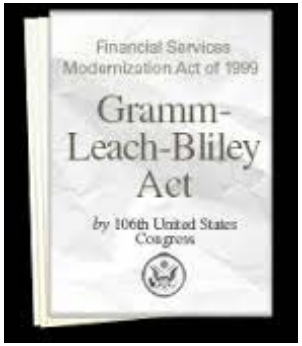
- Identify **what** you have
  - Financials, customers/donors, employees, transactions, intellectual property, legal, technical, trade secrets
- Identify **where** it's located
  - Hardcopy, electronic, on premise/off premise, encrypted
- Confirm **why** you hold onto it
  - Storage, active vs. archive, retention
  - Keep only what you need
- Also identify **who** is responsible for each data type
  - Data governance, ownership, single source

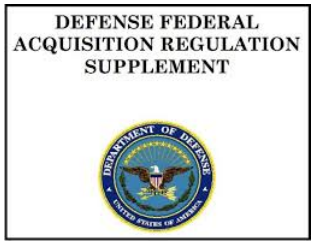
QUESTION #3

Rules and regulations?

ACTION: COMPLIANCE/PRIVACY LANDSCAPE

Information
Security
Forum





EKS&H
AUDIT | TAX | CONSULTING

ACTION: SAMPLE PCI DSS REQUIREMENTS

- Install and maintain a firewall configuration to protect cardholder data.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.

High Risk

Score	Recommendation	Severity	Probability
100	**PCI DSS Requirement 3.2 - Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.** Identify and remove the source resulting in storage of Primary Account Numbers (PAN) in the file system.	High	High

File	Data
C:\Program Files (x86)\Dell\SysMgt\omsa\ini\pcidb.txt	4444********0003
	5333********8901
E:\Shared Folders\IT\Data cubes\AR_slm_cube.xlsx	4899*****9999
	4499*****9998
	4900*****0007

QUESTION #4

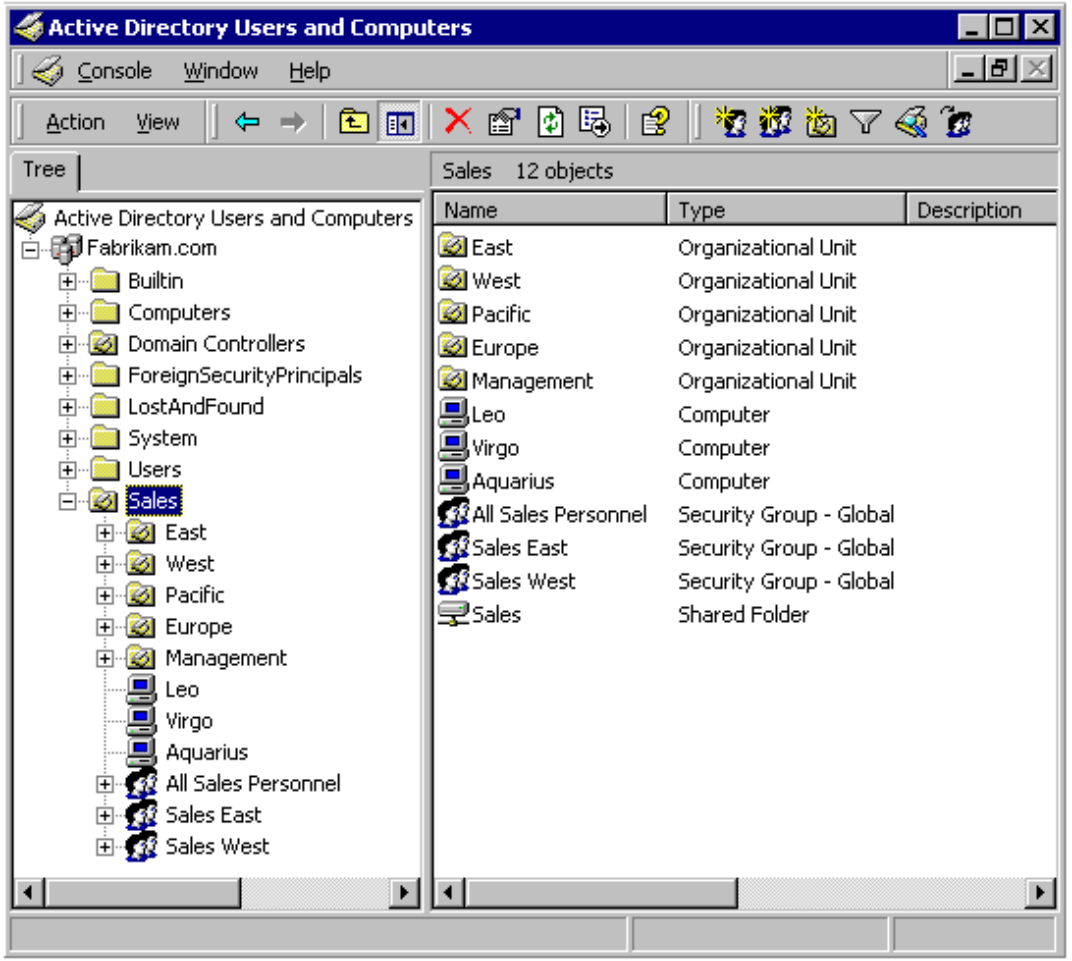
Who has access?

ACTION: USER MANAGEMENT

- Who has access?
- To what information?
- How is access decided?
- How are new users set up?
- How about promotions or transfers?
- What happens when an employee leaves the organization?
- What are the access policies for contractors, vendors, or other business partners?

ACTION: USER MANAGEMENT

- Internal and external systems
- Groups / Roles
- Privileges
- Policies
- Beware of over-granting or duplicating access



Source: msdn.Microsoft.com

QUESTION #5

How is access enforced?

WORST PASSWORDS OF 2016

teamsid.com/worst-passwords-2016

2016 list is based on **over 5 million** passwords posted or for sale on the Internet

RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2 ↗
4	12345678	1 ↘
5	football	2 ↗
6	qwerty	2 ↘
7	1234567890	5 ↗
8	1234567	1 ↗
9	princess	12 ↗
10	1234	2 ↘

EKS&H
AUDIT | TAX | CONSULTING

2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

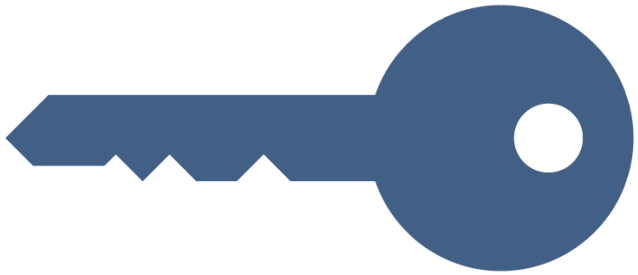
verizon

63% of confirmed data breaches involved weak, default or stolen passwords.

EKS&H
AUDIT | TAX | CONSULTING

ACTION: AUTHENTICATION

- Establish and implement a practical password policy
  - Length, complexity, duration
- Utilize enterprise-grade password management tools
- If Single-Sign-On (SSO) strategy, make it stout
- Concentrate authentication to core business systems
- Consider two-factor authentication
- Trust but verify

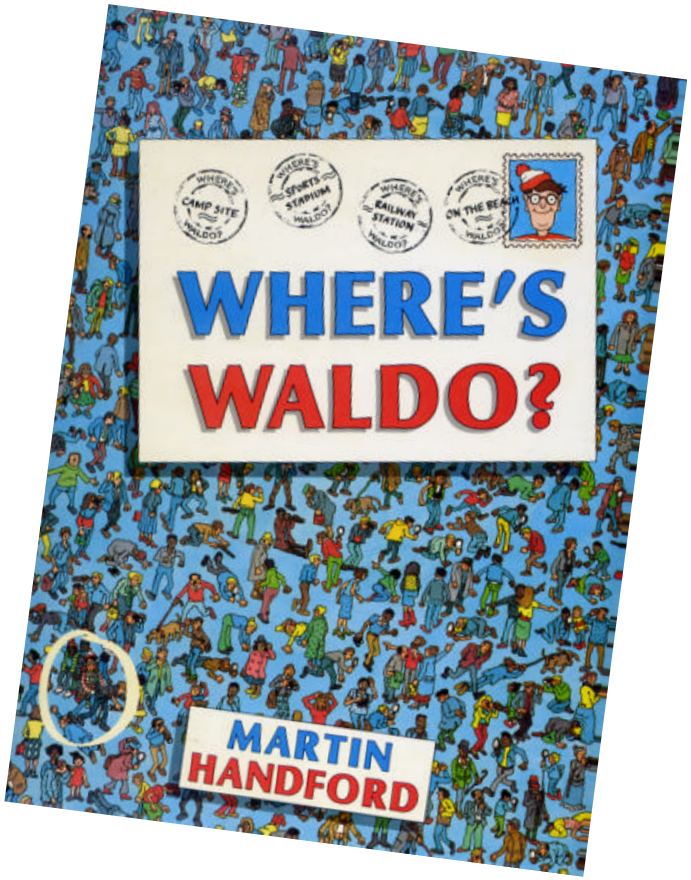


QUESTION #6

Identifying suspicious activity?

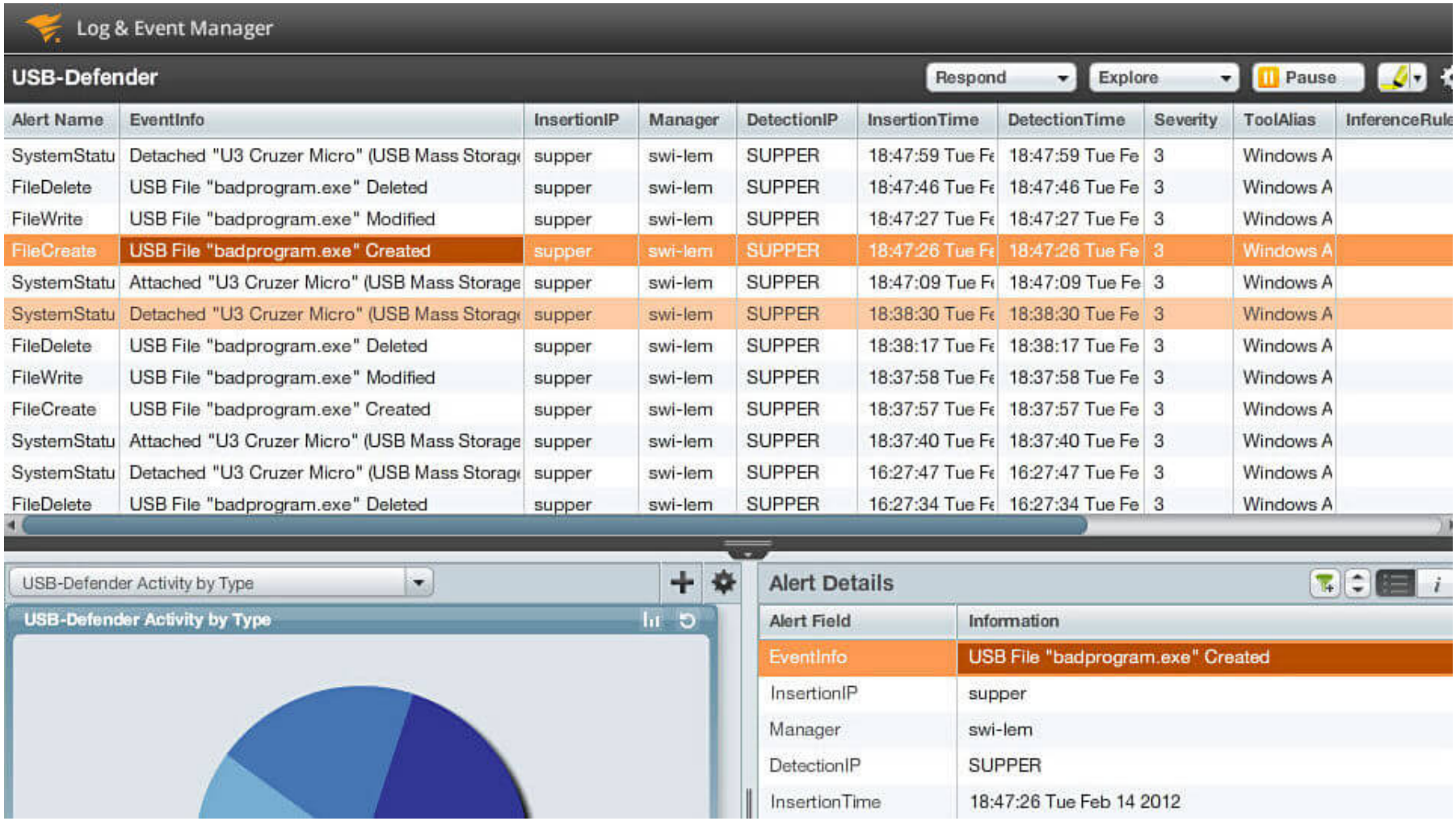
ACTION: MONITORING

- Avalanche of system log data
- Sifting through the noise
- Monitoring Tools
- Advanced Security Analytics
- Managed Security Services



ACTION: MONITORING

Source: http://www.solarwinds.com/kiwi-syslog-server.aspx



EKS&H
AUDIT | TAX | CONSULTING

QUESTION #7

What is my response plan?

ACTION: RESILIENCY

- Have an overall information security strategy.
- For each identified risk:
  - Treat it, transfer it, accept it (or ignore it)
- Conduct periodic vulnerability assessments.
- Adopt, update, and test cybersecurity plans:
  - Backup and restore process
  - Disaster recovery plan
  - System patches and updates
  - Breach response plan

ACTION: BREACH RESPONSE PLAN

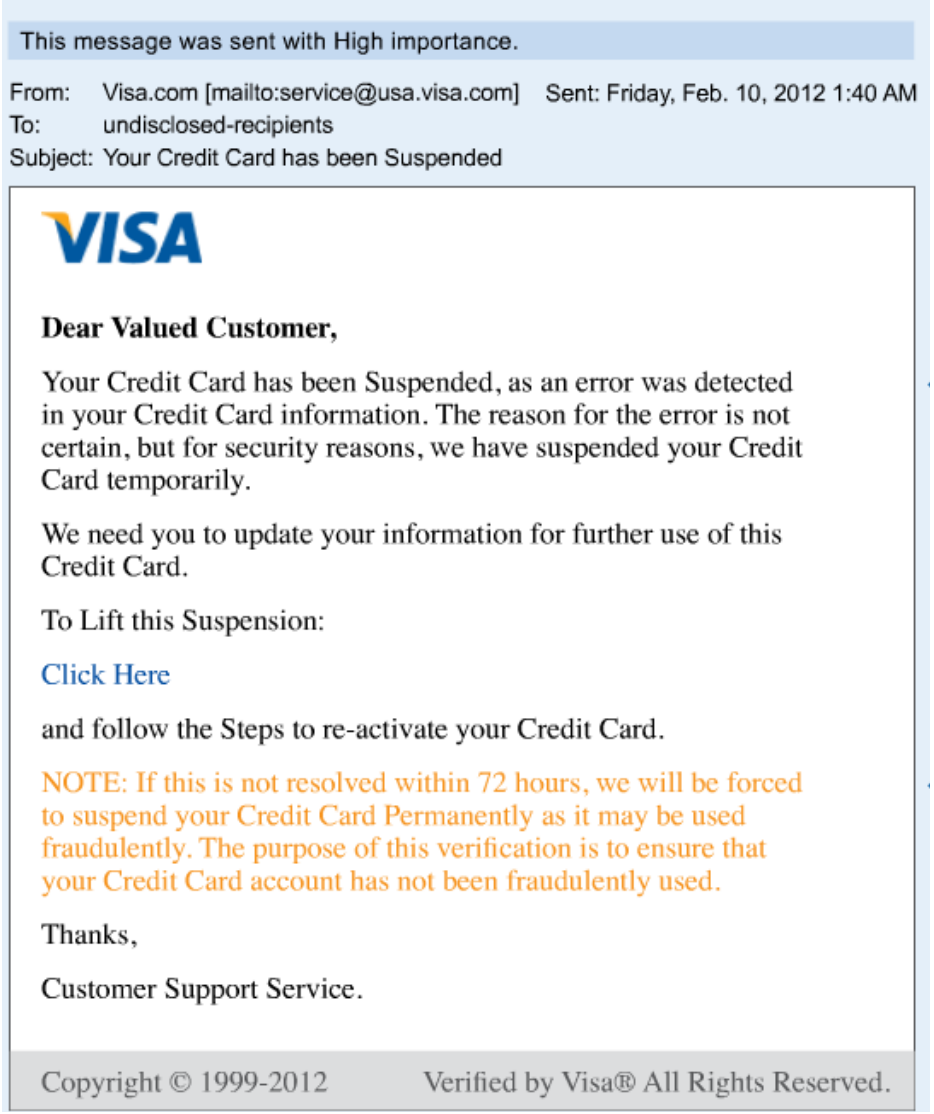
- Definition of a breach
- Breach response teams and responsibilities
- Recovery activities
- Communicating the breach
- Dealing with the breach
- Restoring operations
- Testing and maintenance

QUESTION #8

How susceptible are my employees?

ACTION: SECURITY AWARENESS

How to catch a phish…



This message was sent with High importance.

From: Visa.com [mailto:service@usa.visa.com] Sent: Friday, Feb. 10, 2012 1:40 AM
To: undisclosed-recipients
Subject: Your Credit Card has been Suspended

VISA

Dear Valued Customer,

Your Credit Card has been Suspended, as an error was detected in your Credit Card information. The reason for the error is not certain, but for security reasons, we have suspended your Credit Card temporarily.

We need you to update your information for further use of this Credit Card.

To Lift this Suspension:

Click Here

and follow the Steps to re-activate your Credit Card.

NOTE: If this is not resolved within 72 hours, we will be forced to suspend your Credit Card Permanently as it may be used fraudulently. The purpose of this verification is to ensure that your Credit Card account has not been fraudulently used.

Thanks,

Customer Support Service.

Copyright © 1999-2012 Verified by Visa® All Rights Reserved.

EKS&H
AUDIT | TAX | CONSULTING

ACTION:
SECURITY AWARENESS: SPEAR-PHISHING

From: Curt [mailto:curt.@]
Sent: Thursday, October 29, 2015 4:35 PM
To: Jason <Jason.@the>
Subject: Urgent

Jason,

I need payment sent out.

Kindly let me know when you can have this done so i can forward Account Details to you.

Reply me once you receive this.

Best Regards
Curt
President

is a Top 100 Great Supply Chain Partner Three Years Running!

Read Chains of Command for WMS topics you can use today.

Source: www.technologyassociates.net/avoid-wire-transfer-scam-emails/

ACTION: SECURITY AWARENESS

- *People* are the weakest link in the cybersecurity chain.
- Social engineering and phishing attacks:
  - Users coerced into giving away credentials
  - Redirection to malicious sites through email links
  - Spoofed websites to capture personal or corporate data
- The traditional technology-centered view of cybersecurity is expanding to include people and processes.
- Awareness training may be your most effective investment.

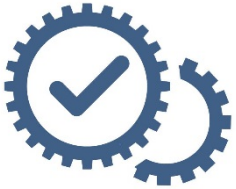
EIGHT-POINT INSPECTION REVIEW

1. Perimeter Defense

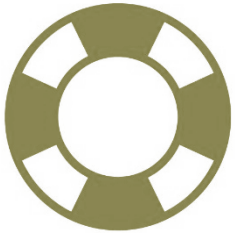
5. Authentication

2. Data Inventory

6. Monitoring

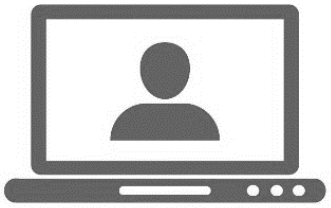


3. Compliance



7. Resiliency

4. User Management



8. Awareness

EKS&H
AUDIT | TAX | CONSULTING


Questions?
9
EKS&H
AUDIT | TAX | CONSULTING

Thank you!

Dan Domagala | ddomagala@eksh.com

EKS&H
AUDIT | TAX | CONSULTING