SECURITY IN A TECHNOLOGICAL AGE

By Rick Shaw, CEO/Founder Awareity

Background of Rick Shaw….

- Supported over 400 banks with security, privacy, disaster recovery, risk management, compliance and more.

- Designed communications and information security/privacy solutions for all types and all sizes of clients.

- Founded CorpNet Security in 1998 and delivered risk, vulnerability and compliance assessments for all types and all sizes of clients.

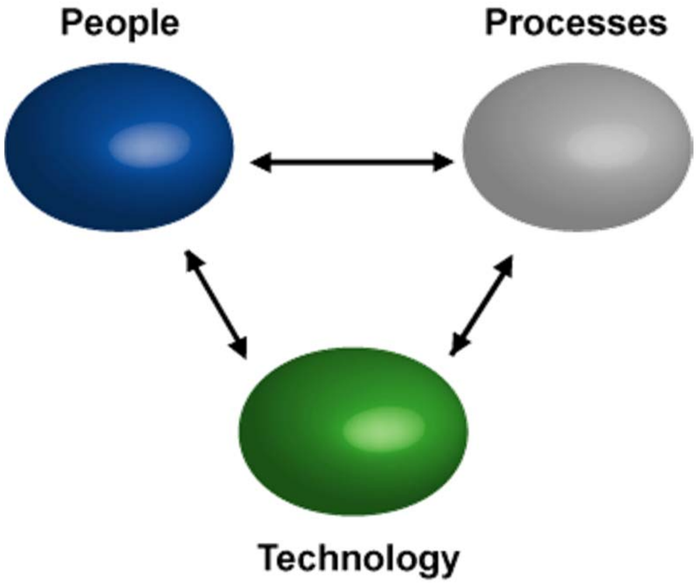
- Founded Awareity in 2004 because better solutions and better tools were needed to eliminate expensive gaps and disconnects associated with the weakest link(s) in every organization.

Learning Objectives

- Examine examples of information security/privacy risks
- Review technological, procedural and people related security issues faced by financial institutions
- Explore the latest technologies and threats with regard to information security and privacy
- Understand the information security requirements as defined by numerous regulations and national standards

Connecting the Dots
Requires Managing Key Components

Technology Receives the Most Attention and $$$$$



Technology

- *Firewalls, AntiVirus*
- *Tokens, Authentication*
- *IDS, IPS, DLP, Filters*
- *Application / DB*
- *Intranets*
- *E-mail / Text Messaging*
- *LMS / Knowledge Centers*
- *Mobile Devices / Phones*
- *Social Networks (Twitter)*
- *And lots of other Dots too…*

Processes

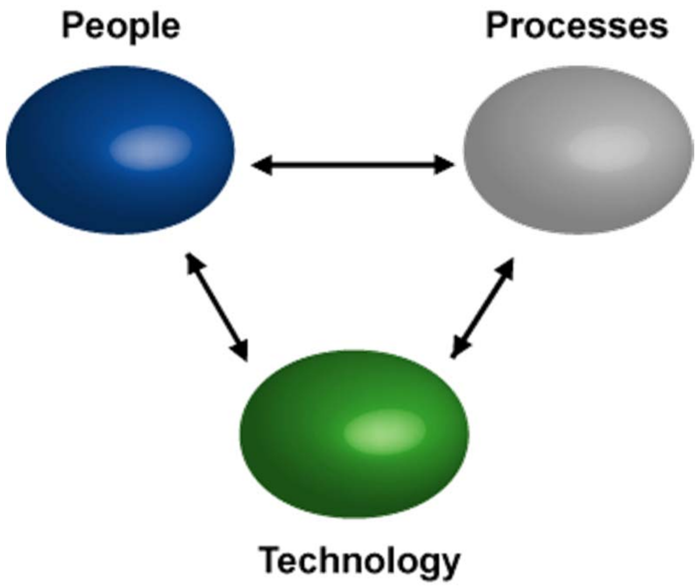
- *Plans*
- *Procedures*
- *Policies*
- *Roles*
- *Responsibilities*
- *Checklists*
- *Guidelines*
- *Priorities*
- *Strategies*
- *Organizational Training*
- *Code of Conduct Manuals*
- *Assessments*
- *And lots of other Dots too…*

People

- *Employees*
- *Management*
- *Customers*
- *Board of Directors*
- *Contractors/Vendors*
- *Law Enforcement*
- *Risk Management Team*
- *Audit Committees*
- *Media*
- *Legal*
- *Human Resources*
- *IT*
- *And lots of other Dots too…*

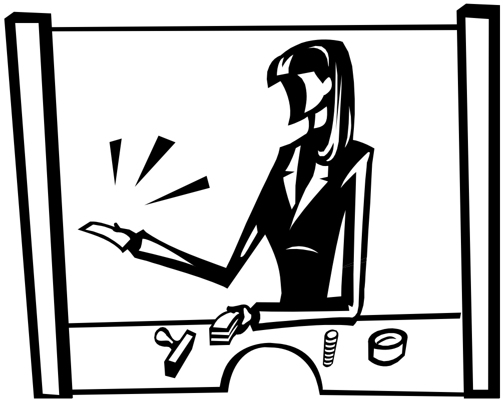
Connecting the Dots and Eliminating Gaps Requires Managing Key Components

Which is the weakest link?



Where are “Bad Guys” focused?

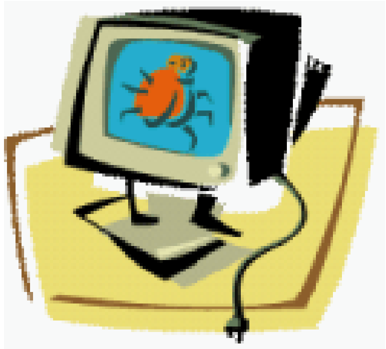
- Attacks are focused at People!
- Attacks focused at People are becoming more sophisticated
- Attacks focused at Processes (that People are not following)



Bad guys know it is easier to hack people and processes than firewalls and technology.

Technology?

- ✓ *How many organizations have AntiVirus Software?*
- ✓ *How often is AV updated? Why?*
- ✓ *How easy is it to verify AV software is updated?*
- ✓ *How often do you check?*
- ✓ *How much do you pay for AV software and maintenance?*



Technology?

- ✓ *How many organizations have a Firewall?*
- ✓ *How often is your FW updated?*
- ✓ *How easy is it to verify FW is updated?*
- ✓ *How many have an ongoing vulnerability assessment service? Why?*
- ✓ *How often do the vulnerability assessments run?*
- ✓ *How much do you pay for the vulnerability assessments?*
- ✓ *How much did you pay for the FW?*
- ✓ *What is your cost per User? (Total Technology/# of people)*

Technology?

- ✓ *How many organizations have Security (physical) alarms/cameras?*
- ✓ *How much do you pay for people to monitor?*
- ✓ *How much do you pay for maintenance?*
- ✓ *How many organizations have IDS, IPS, DLP, Anti-Spyware, etc.?*

Is it safe to say organizations have made significant investments in technology solutions?

Processes? (Recipes)

- *Plans*
- *Procedures*
- *Policies*
- *Roles*
- *Responsibilities*
- *Checklists*
- *Guidelines*
- *Priorities*
- *Strategies*
- *Organizational Training*
- *Code of Conduct Manuals*
- *Assessments*
- *And lots of other "Dots"…*

People?

- *Employees*
- *Management*
- *Customers*
- *Board of Directors*
- *Contractors/Vendors*
- *Law Enforcement*
- *Risk Management Team*
- *Audit Committees*
- *Media*
- *Legal*
- *Human Resources*

How often do you update and check your people?

The Power of Focus

Are your "People" prepared to prevent latest attacks?

Is your organization in compliance with each regulation/mandate that applies to your organization?

Do all "People" have updated situational awareness?

How are you "connecting all the right dots"?

Do you have a way to get all of the right Processes to the right People so they know and can do the right Things?

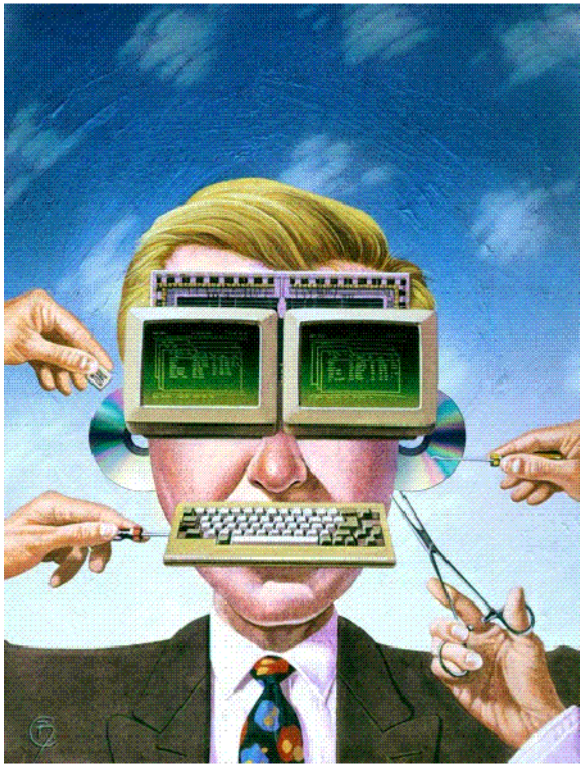
www.AWAREITY.com

The Secret with People…USB Port??

*To be effective, Anti-virus software must be **implemented** on all devices, **updated** as new risks and threats occur, and **monitored** ongoing.*

*To be effective, situational awareness must be **implemented** across all individuals and individuals must be **updated** as new risks, new threats, and challenges arise.*

*Individual acknowledgements and accountability must then be **monitored**, measured, tracked and documented.*



Dangerous and Costly Trends….

- Phishing E-mails are More Sophisticated
- Malware is Showing Up in More Places…
- Lawsuits/Settlements are Increasing
- Fines are Increasing
- Regulations are Mounting
- Insurance Costs are Rising
- Workplace Violence is Increasing
- Threat of Terrorism is Closer to Home
- Data Breaches Continue to Occur
- Costs of Data Breaches Are Significant
- Insider Threats Are Real
- Losing Customers is Expensive

The Secret to Change…

The only permanent thing known to man is change.

The secret to change for bankers is continuously updating your People (weakest link) as well as your Processes and your Technology.

Hackers are changing their tactics every day…are you?

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Identity Theft #1 Concern

FACTA Red Flags Program (one of many)

- Does your organization have policies and procedures in place?
- Identity Theft #1 Concern among bank customers
- #1 Cost is Lost Business

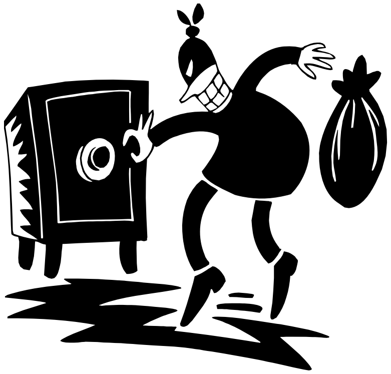
Incident Reporting

- How do your employees report Red Flags?
- Do your customers understand how to report incidents?

Identity Theft is one of the fastest growing crimes in the U.S. with over 10 million victims a year.

Cyber Attacks, Identity Theft, Phishing, Spyware, Keyloggers and Social Engineering

- What is Phishing?
- What is Spear Phishing?
- What is Spyware?
- What are Keyloggers?
- What is SPAM?
- What is Social Engineering?



Bad Guys go where the money is…

(banks and customers…and vendors)

Bad Guys attack your weakest links…(employees & customers)

www.AWAREITY.com

Case Study: Phishing

Group Discussion:

You become aware that several employees (maybe all) have received an e-mail that looks like it is from one of your executive managers asking employees to click on the link in the e-mail to ensure that your new Disaster Recovery plan has everyone's updated contact information and system login information in case employees are forced to work from home during a disaster.

But…your executive manager did not send the e-mail.

This is a phishing attack on your bank, now what?

Cyber Security vs. Physical Security

What would happen if someone sent a phishing e-mail to a bank employee…what would they do?

What would happen if someone was asking questions about the bank or employees on social media?

What should your employees do according to your policies and security processes?

Physical Security

What would happen if someone walked into your bank and they were wearing a long trench coat and started taking pictures of the inside of your bank…what would you do?

What should your employees do according to your policies and security processes?

Phishing Attacks on the Rise

Phishing messages accounted for 17% of all spam.

- Takes advantage of economic challenges, natural disasters, politics, etc.
- More malware in 2007 than previous 17 years combined…and STILL increasing
- Cyber thieves are creating thousands of new pharming sites every week to exploit popular brands like Amazon, eBay, PayPal, Visa, Bank of America, etc.

How are you keeping your employees and customers aware?

RSA Data Breach

Advanced Persistent Threat Attack

□ RSA employees were targeted with a **spear phishing** attack and at least one employee made the mistake of clicking on the attached Excel spreadsheet, which targeted a zero-day vulnerability in Adobe Flash.

□ Attackers stole information for 40 million two-factor authentication accounts.

□ Expensive, Embarrassing and Loss of Customers

Data Breaches - Bottom Line Costs

Data breach average costs to organizations are just under $4M and you can view data breaches since 2005 at www.privacyrights.org

Data breach costs are about $200 per record.

In addition to expensive costs, organizations face the threat of lawsuits from employees or customers whose personal information is mishandled or stolen.

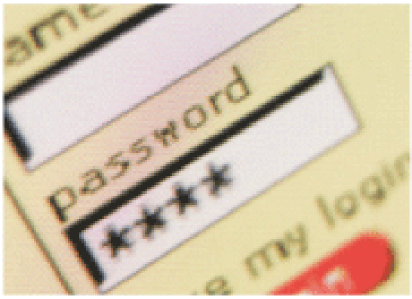
What is Pharming?

Pharming: when a users types in a valid URL but is redirected to a website designed to collect personal information

Drive-by Pharming

- Home routers left with default login and password
- Point User's browser to fraudulent bank site

SPAM e-mails



- According to a recent Messaging Anti-Abuse Working Group (MAAWG) survey, tens of millions of users continue to respond to spam in ways that could leave them vulnerable to a malware infection or bot network.

- Nearly half of the users have opened spam, clicked on a link in spam, opened a spam attachment, replied, or forwarded it-all activities that leave consumers susceptible to fraud, phishing, identity theft, and infection.

Social Engineering…and how to spot it.

What is Social Engineering?

Manipulating people into performing actions or divulging confidential information

Wal-Mart Example

Social engineer used gift card numbers to steal $11,000 in online merchandise

Bank Example

A man dressed as an armored truck employee walked into a bank and was handed more than $500,000 in cash… It wasn't until the actual courier arrived at the bank the next day that bank officials realized they'd been had…

Could this happen at your bank?

Are all employees aware?

During an assessment of a financial organization’s security, a security firm randomly placed 20 USB thumb drives through the organization’s office, lunch room, restrooms and reception area. All drives were loaded with one file that appeared to be a picture.

Fifteen of the drives were picked up by employees, who promptly loaded them into their computers and attempted to open the file.

The file was actually a Trojan horse virus, which sat hidden in the computer system collecting account numbers. After two days, 80% of the account numbers were captured and the information was e-mailed to the security firm – unknown to anyone at the organization.

This is called “Baiting”

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Risks of Social Media

Cybercriminals are moving aggressively to take advantage of social networks and social media in workplace settings.

- Facebook – example of how hackers are using social media
- Twitter – example of how hackers are using bitly links
- LinkedIn – example of how hackers are using

Does your organization have a social media policy in place? Do you employees understand the dangers of posting personal/organizational information? Are employees aware of social media risks? How many of you give a way clues to your passwords?

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Customer Awareness

- Most recent FFIEC guidance stresses the need for performing risk assessments, implementing effective strategies for mitigating identified risks and raising customer awareness of potential risks

- Key recommendation for eliminating fraud is customer awareness and education.

- The main reason customers don't move to mobile banking is because of security concerns. ***"Only 17 percent of financial institutions are educating their customers about mobile malware and anti-virus software."***

Customer Awareness

- 67% of bankers say customer awareness is the best way to prevent fraud
- Surveys show more than 75% of financial institutions learn of fraud incidents when notified by their own customers

How is your organization expanding your customer awareness?

- Mailings
- Seminars
- Online Awareness and Alerts for Customers
- Incident Reporting for Customers
- Policy Acknowledgements for Customers
- Legal Due Diligence and Documentation

Information Security Awareness is Critical

- **Customers are the focus/target of more sophisticated threats**
  - Phishing, Spear Phishing & Pharming
  - Social Networking & Curiosity
  - Keyloggers and Spyware

- **Processes are as/more important as Technology**
  - Information Handling (laptops, desk tops, etc.)
  - Information Sharing (vendors, users, responders, etc.)

Connecting the Dots helps eliminate/prevent gaps

- Physical, Cyber, Home, Wireless, etc.
- Situational Awareness as Risks and Threats Change

Are your Customers Aware?

- Swedish bank Nordea was stung for **$1.1 million**—one of the "biggest ever“ online bank heists.
- 250 customers were affected by the fraud, after falling victim to phishing e-mails
- Customers were redirected to a false home page, where they entered important log-in information, including log-in numbers
- Most of the customers affected had not been running antivirus applications on their computers. The bank has borne the brunt of the attacks and has refunded all the affected customers.

Awareness or Technology problem??

Customers Targeted Here Too….

- Customers receive text messages asking for personal banking information
- Says debit card has been inactivated… give number to call to reactivate
- Those who provide information… instantly have their bank accounts wiped out

In the Broken Bow scam, scammers sent an automated telephone message to mobile phones with Broken Bow area prefixes. The message identified the caller as Nebraska State Bank and states there is a problem with a customer's debit card. It requests responses by either calling a certain number or typing information directly into the phone.

Would your Bank's Customers know what to do?

ACH/Corporate Accounts

- Online banking fraud involving the electronic transfer of funds has been on the rise since 2007
- Attacks by hackers have hit both private businesses and government entities with fraudulent wire transfers ranging from $100,000 to $500,000 and more
- Almost all CA incidents reported to the FDIC involved malware on the customers' PCs they used for online banking. (phishing emails, etc.)
- Rather than just taking small amounts of money via ACH transactions, they wire large amounts of money overseas.

ACH/Corporate Accounts and Lawsuits

Unknown attackers initiated a series of unauthorized wire transfers for over $800,000 from Hillary Machinery, Inc., Hillary demanded their bank repay the stolen money. The bank filed a lawsuit against the customer stating that its security procedures were “commercially reasonable.” Then the bank sued their customer.

In this incident, unauthorized wire transfer orders were placed by hackers using the valid Internet banking credentials of the customer. The customer insists it was the bank’s failure to implement strong authentication and fraud-detection measures that enabled the theft. Numerous red flags included:

- Money was being transferred to foreign destinations (which had never happened before)
- Dozens of transactions were made in a 2-3 day period
- Sums of the transfers were outside the normal range of the customer
- Each of the transfers was made to a different account
- Bank received two e-mail requests to register other computers on the customer’s behalf (e-mails were sent from the customer’s e-mail address, but the IP addresses were based in Italy and Romania)

ACH/Corporate Accounts and Lawsuits

Hillary Machinery – Court ruled in favor of Customer because the bank did not have or follow commercially reasonable security measures in place and led to a settlement

PATCO – Court ruled in favor of Customer because the bank did not implement commercially reasonable security measures and led to a settlement

Choice Escrow Land Title – Court ruled in favor of Bank because the Customer refused dual control authorization offers from the bank

ACH/Corporate Accounts Attack

DDoS Attack with Corporate Account Takeover

DDoS attacks as a cover for customer account attacks?

On a recent Christmas Eve a regional California bank was under DDoS attack and they found out later that Ascent Builders lost $900K and there were 62 individuals that acted as "mules" to receive a deposit from the thieves and then transfer the bulk of the deposits overseas.

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Implementing Lessons Learned…

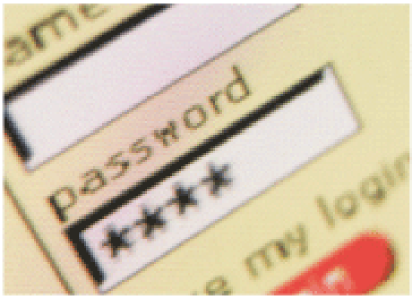
Lessons Learned are valuable only if you connect the dots AND they become Lessons Implemented at the Individual-Level.

It only takes one…

- One individual’s bad decision
- One click on one infected link
- One opened attachment
- One lost laptop
- One mis-configured technology device
- One negative headline and loss of reputation

…to quickly understand how valuable situational awareness at the individual level is to your bank and customers.

Do you have Weak Passwords?



- Weak passwords really do make hackers’ jobs much easier
- “Forgot Your Password” link info can be obtained from personal blogs, online resumes and social networking sites (Vice-Presidential nominee Sarah Palin hacked)
- Symantec survey revealed 23% of people use their browser to remember passwords
- 60% fail to change their passwords regularly
- 8% used the same password on all their online sites

Does your organization have a Password Policy that explains how strong passwords are created and why passwords are needed?

Case Study: Mobile Security

Group Discussion:

One of your employees was issued an organization-owned laptop/tablet/mobile for use from home and when away from the office. The laptop/tablet/mobile had sensitive and confidential information for both employees and customers due to this employee's work responsibilities. The employee calls the bank and says their laptop/tablet/mobile has been stolen or lost…either way it is gone.

What do you do?

Ex-Employees

A Gucci network engineer, who was fired for "abusing his employee discount," allegedly deleted several virtual servers, shut down a storage area network and deleted corporate mailboxes.

He created a non-existent employee (prior to his being fired), issued the fake worker a VPN token and then "tricked" IT staff into activating it.

Does your organization disable logins when employees leave?

Case Study: Information Disposal

Group Discussion:

You are leaving work after hours and notice two individuals are sorting through the trash bins outside your organization. They see you and quickly leave so you decide to take a look to see what they were doing and you see some of the documents in the trash bin look like they contain sensitive customer information.

OK, Then What?

Lessons Learned: Information Disposal

A janitor was arrested for removing boxes of records from a Southern California health care clinic. Interested only in getting money for the paper, the janitor sold 14 boxes of patient records to a recycling center for $40.

- □ Don't leave sensitive files/information on your desk.
- □ Properly dispose of/shred sensitive information. Don't just toss documents in waste or recycling bins.
- □ Lock and secure file cabinets containing personally identifiable information.

CVS/pharmacy
for all the ways you care

…Expensive Trash

- Employees throwing away pill bottles with personal information
- FTC Investigation – Implement an Information Security Program
- HHS Investigation – HIPAA Violation - $2.25M Settlement
- **Lessons Learned -** 1 Year Later - Rite Aid - $1M Settlement
- What is the Biggest Risk?

The cost of prevention is much less than the costs of recovery.

Your Top Priorities in 2015

- Cyber Attacks, Identity Theft, Phishing, Pharming, Spyware, Keyloggers and Social Engineering
- Social Media Usage and Social Media Risks
- Financial Security Incidents, Case Studies & Lessons Learned
- Customer Awareness to Prevent Fraud and Corporate Account Takeover
- E-mail Security and Privacy Including Anti-Virus and Spam
- Making Policies and Awareness Work Where Technology Fails
- Risk Management Assessments & Vulnerability Assessments

Risk Assessments & Vulnerability Assessments

What is your bank's process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes?

- Do you have Strategies (top down)?
- Are Responsibilities assigned to all appropriate people?
- Are you testing your strategies, technology, processes and people?
- Are you monitoring new risks, threats, technology, processes and people?
- How are you assessing technology, processes and people?
- Are your risk and vulnerability assessments ongoing?
- Are you documenting your assessments and findings and changes?
- Are you automating manual processes?
- Are you updating situational awareness as situations change?
- Are you surveying your people and customers to get their feedback? *(you don't know what you don't know until you ask…)*

Threats - Smishing and Vishing

Smishing :

Victims receive SMS (text) messages along these lines: "We’re confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order on this URL: www.?????.com.“

When visiting the URL, victims are prompted to download a program which turns out to be a Trojan horse.

Vishing:

Criminal practice of using social engineering and Voice over IP (VoIP) to gain access to personal and financial information for the purpose of identity theft.

Vishing exploits the public's trust in landline telephone services. The victim is often unaware that VoIP allows for caller ID spoofing, complex automated systems and anonymity for the bill-payer.

Risks and threats are constantly evolving with new ‘technology’ and becoming more sophisticated.

Evolving Threats…Always Changing

Clickjacking - An attacker slips a malicious button/link onto a legitimate web page so when visitors are clicking on the buttons they are actually clicking on a link the attacker has placed on the web site.

Tab napping - Targets Internet users who open several tabs on their browser at the same time. Hackers will replace an inactive browser tab with a fake page set up specifically to obtain personal information. Once you have opened a new tab and visited a web page, that initial web page does not necessarily state the same if you don't return to it for a time while you use other windows and tabs. Malicious code replaces the web page you opened with a fake version which looks identical to the legitimate page you originally visited.

Typo-Squatting - Relies on typographical errors made by Internet users when typing a website address into the browser. If a user accidentally enters an incorrect address, they are led to an alternative website owned by a cybersquatter.

It only takes one…

- One individual's bad decision
- One click on one infected link
- One opened attachment
- One lost laptop
- One mis-configured technology device
- One negative headline and loss of reputation

…to quickly understand how valuable situational awareness at the individual level can be to your bank and customers.

FREE Educational Resources

Organizations can access Awareity's educational services free of charge to review recent blogs, news, success stories and other resources at www.awareity.com.

CONNECTING THE DOTS BLOG

follow us on twitter

Financial

Questions or Comments?

Rick Shaw

info@awareity.com

www.AWAREITY.com