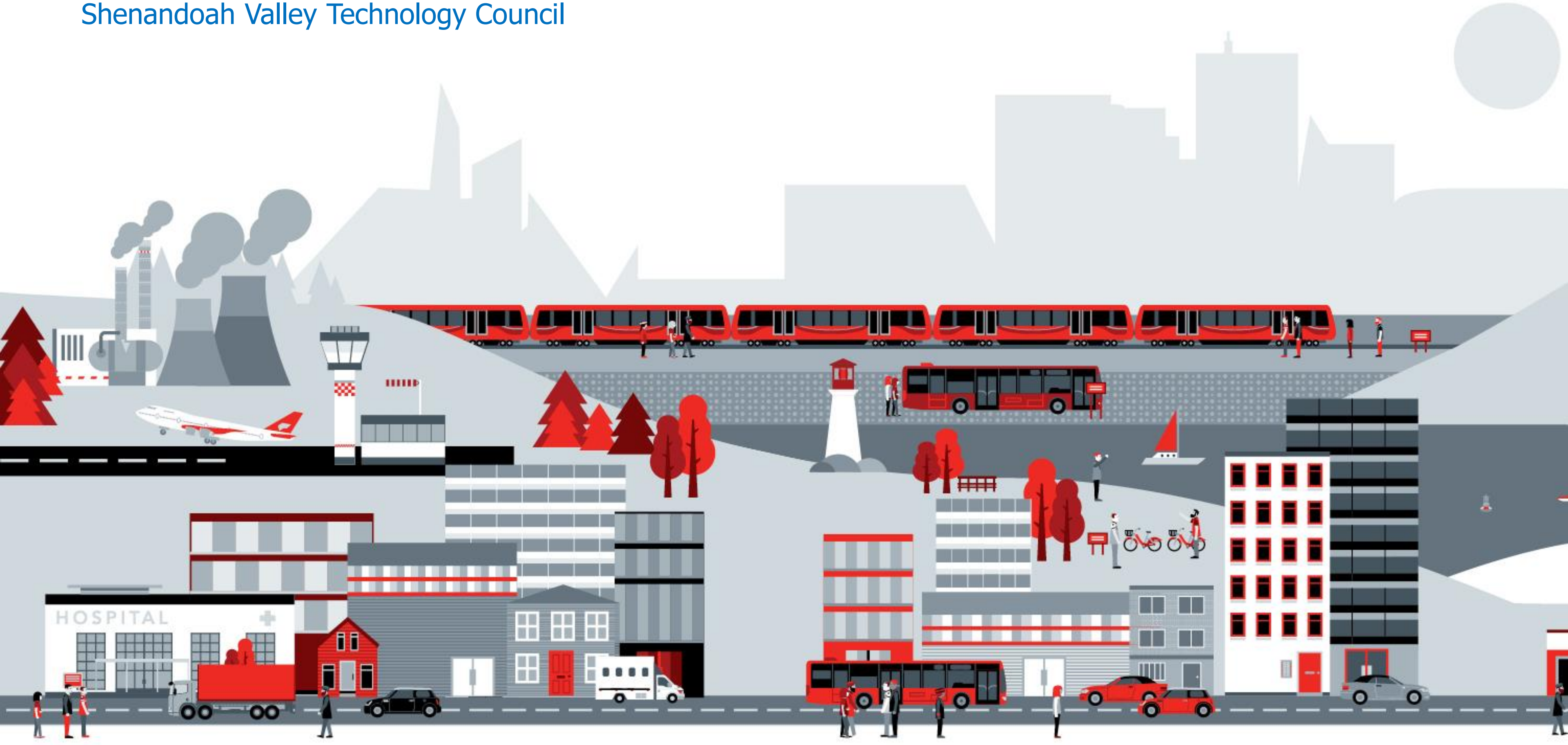
SHENANDOAH VALLEY TECHNOLOGY COUNCIL
For technology users and creators

serco

Anatomy of an Attack
Cyber Threats Facing CIOs and How to Defend Against Them

Cyber Security Awareness For Businesses 2.0

Shenandoah Valley Technology Council



Agenda

Cyber Security – What's the Big Deal?

- Common Cyber Misconceptions
- Interesting Cyber Statistics

Preparing An Effective Cyber Defense Plan

- One Size Does Not Fit All
- A Multi-Layered Approach
- Training, Awareness & Testing
- Understanding Different Types Of Attacks
- Why Is Phishing So Successful
- Know Your Enemy

Detection And Response

- How Do You Know If You've Been Hacked

Remediation

- Once They're In, How Do You Get Them Out

How Do You Know When You're Done

- When Do You Have Enough Protection

Cyber Security Awareness For Businesses 2.0
Shenandoah Valley Technology Council

> *"There's two kinds of CIOs: ones who have been hacked and know it, and those who have been hacked and don't yet realize it. But the reality is, you've been hacked."*
>
> - Tony Scott, Federal CIO of the United States
>
> *Former CIO of VMWare, Microsoft, and The Walt Disney Company*

Cyber Security

What's the big deal?

Common Cyber Misconceptions

A Common CEO Misconception:

"I spend a fortune on Cyber Security. There's no way I'll get hacked!"

The reality is:

- Throwing money at a Cyber program is not enough
- An effective Cyber program must be well thought out and planned – your environment, the type of data you are protecting, and the level of cyber training and awareness of your employees will greatly influence your cyber strategy.

A Common End User Misconception:

"I only open and read emails from my friends and business colleagues to make sure I don't get infected with any malware."

The reality is:

- Hackers will spoof the email addresses of your friends and colleagues to make you think the emails are coming from them
- Phishing email are becoming so sophisticated it is becoming very difficult to tell the difference between a real email and a malicious email – *constant employee training and awareness is key*

Cyber Security
What's the big deal?

Common Cyber Misconceptions

A Common IT Manager Misconception:

> *"I make sure all my end users have up to date anti-virus software and definitions, so we're safe from being hacked"*

The reality is:

- Up-to-date anti-virus/anti-malware software and definitions won't stop Zero-Day Exploits or some phishing emails
- While it helps, up to date anti-virus software and definitions are only a small portion of a effective cyber strategy

A Common Small Business Misconception:

> *"I'm a small regional business. Who would hack me?"*

The reality is:

- Hackers often look for small or medium sized businesses with an Internet presence in order to compromise their systems to use as attack jump-off points or cyber extortion *(ramsomeware)*
- Small businesses are often more attractive to hackers because they believe they are less prepared to defend against an attack

Cyber At A Glance

Interesting Statistics Related to Cyber Attacks

48%

The increase in reported incidents in 2015, with an avg. of 117,339 attacks per day

Source: "The Global State Of Information Security Survey - 2015" | PWC

169million

Number of personal records exposed in 2015 as a result of security breaches

Source: "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC

$154.00

Avg. global cost of a lost or stolen record containing confidential and sensitive data

Source: "Cost of Data Breach Study: Global Analysis" | IBM/ Ponemon

62%

The number of cyber victims who are small and medium sized businesses

Source: Timothy Francis, Travelers Insurance

38%

Percent of global organizations that claim they are prepared for a sophisticated cyber attack

Source : "2015 Global Cybersecurity Status Report" | ISACA International

200days

The average amount of time an attacker remains dormant in a network before detected

Source: "Microsoft Advanced Threat Analytics" | Microsoft

Why is this important? Because every business, regardless of size, revenue, or industry is a potential target of cyber criminals and should prepare accordingly

Preparing An Effective Cyber Defense Plan

One Size Does Not Fit All

There are several unique characteristics to each business that will help shape an effective cyber security plan, including:

1. The industry/business you are in….
   - A company that designs and manufactures classified weapon systems for the US DoD will have a different plan from a company that sells office supplies over the Internet
2. The size and kind of technology you leverage to run your business….
   - A nuclear power plant will have a different plan as compared to a local hardware store
3. The level of cyber security awareness within your workforce….
   - Attackers are targeting end users first, relying on their lack of cyber training and awareness to "click" on the wrong thing

The one constant that should be included in every plan is a *Cyber Training and Awareness* program for all employees

- Think of your employees as your first line of defense, and train/condition them to recognize threats
- Establish a culture where cyber security is the responsibility of ***every*** employee, and not just the IT Dept

Preparing An Effective Cyber Defense Plan
A Multi-Layered Approach

A good Cyber Defense Plan Will have Multiple Layers – *Defense in Depth*

As a guideline, 6 Layers of a good Cyber Defense Strategy should include:

1. Your Employees
   - Regular recurring Cyber Training & Awareness to ensure that security remains top of mind
   - Engrain cyber awareness into the culture of the workforce, without this the rest of your plan could be rendered ineffective
   - Considering building an internal InfoSec team capability if cyber defense is a 24x7 issue affecting the success of your business
2. Your Data / Intellectual Property
   - Classify data based on business sensitivity and separate low value from high value assets so you know where more rigorous protection measure need to be - avoid building *"Digital Landfills"*
   - Establish roles/personas within your workforce and define which roles have what level of access to the different information/data within your network
   - Employ strong & complex passwords to access your data – the longer the better
   - Consider using data encryption tools on your high value assets, for both data at rest and data in motion
   - Consider using PKI Certificates / multi factor authentication for more advanced protection of assets
3. Your Systems / Applications
   - Conduct security vulnerability assessments & penetration tests on a recurring basis to test/validate your configurations
   - Develop a mature Configuration Management process for protecting against unauthorized changes
   - Consider using a Secure Application Gateway for user authentication and access to your critical systems / applications
   - Role / Persona based user access with PKI Certificates / multi factor authentication

Preparing An Effective Cyber Defense Plan
A Multi-Layered Approach (cont.)

A good Cyber Defense Plan Will have Multiple Layers – Defense in Depth

As a guideline, 6 Layers of a good Cyber Defense Strategy should include:

4. Your Endpoints (Desktops/Laptops/Tablets/Mobile)
    - Centrally managed endpoint security (anti-virus, anti-Malware, desktop firewall, patch mgt, hard drive encryption, intrusion detection & prevention)
    - Application whitelisting so only approved apps can run on the endpoint
    - Consider removing local administrative privileges, locking down USB desktop/laptop ports where possible
5. Your Network & Data Center
    - Implement network enclaves / protected network segments to isolate network traffic
    - Enterprise Network Access Control & Secure Wi-Fi Access to prevent unauthorized access on your network
    - Advanced message security / email filtering as a more effecting way to block phishing emails
    - Web proxy / content filtering to restrict Internet access from hitting known compromised websites
    - Secure remote access / VPN using multi-factor authentication
    - Consider deploying Data Loss Prevention (DLP) tools to prevent unauthorized data leakage
6. Your Perimeter
    - Enterprise Perimeter firewalls, Intrusion Detection & Prevention, Secure DMZs, Perimeter based DLP

Preparing An Effective Cyber Defense Plan

Training, Awareness, & Testing

Employee Training & Awareness

- This is one of the most critical components of your Cyber Defense Plan, regardless of what business you are in
- Builds a culture of cyber awareness
- Ensures that your employees recognize the various threats, attack types and techniques, and are able to spot them before clicking on something they shouldn't
- Quarterly training (can be CBT or Classroom) is an effective way to make sure your employees are aware of new trends or techniques
- Posting regular communications (emails, posters in breakrooms) warning employees of the pitfalls and risks will keep the topic in the forefront of their thoughts – *top of mind cyber awareness*
- Educate users on how to safely use social media in the workplace
- Regular/frequent "phishing" tests are an effective way to condition employees to recognize and make the right choice

Preparing An Effective Cyber Defense Plan

Understanding Different Types of Attack

There are some interesting correlations between the types of attacks on the increase and the types of assets being attacked

- *There's an ever increasing use of malware to establish back doors that are then exploited by hacking*
- *The primary delivery mechanism of the malware is via phishing emails, taking advantage of an increasing population of victims who are willing to "click" on something they shouldn't*

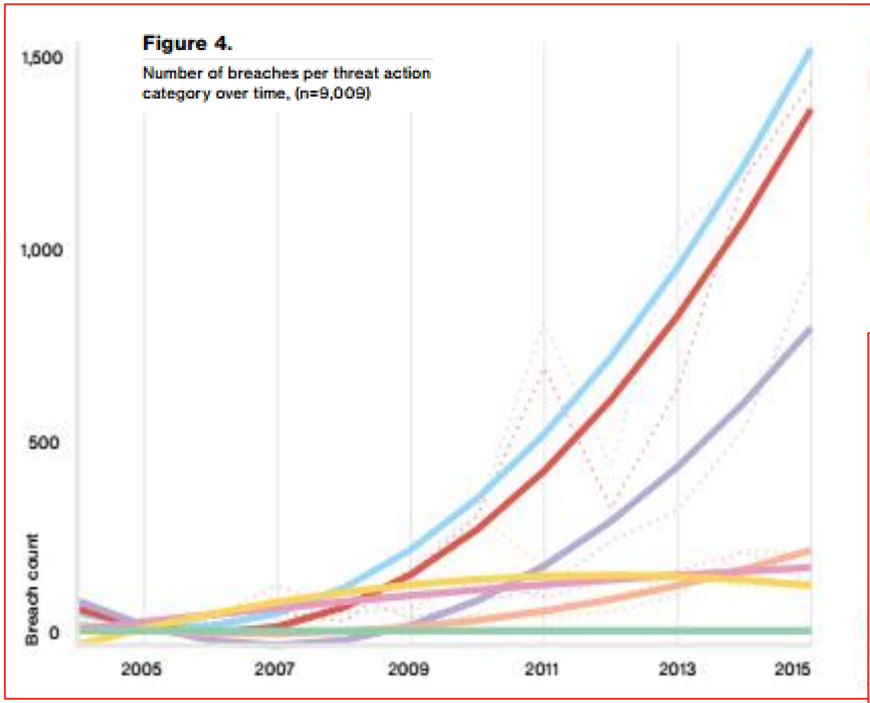


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

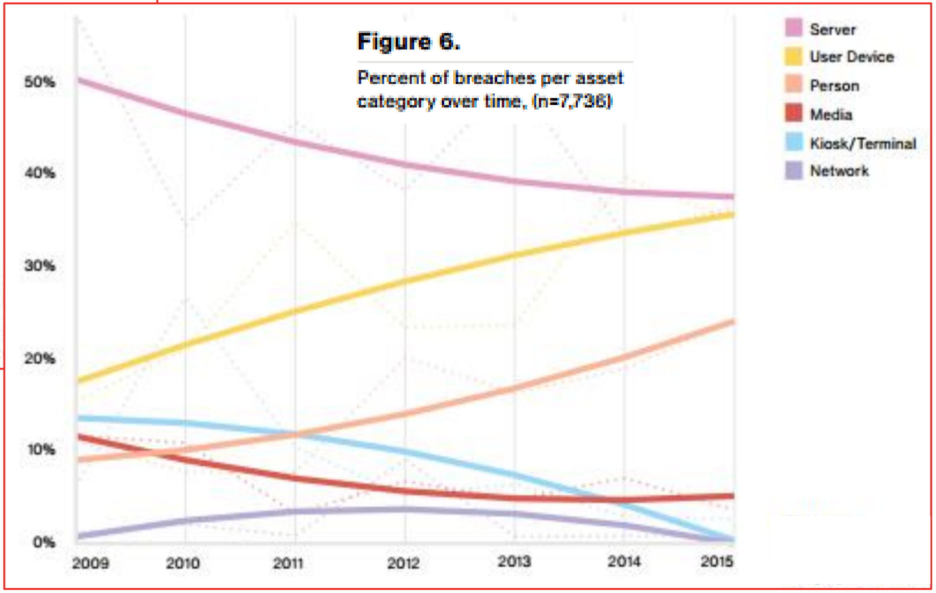


Figure 6.

Percent of breaches per asset category over time, (n=7,736)

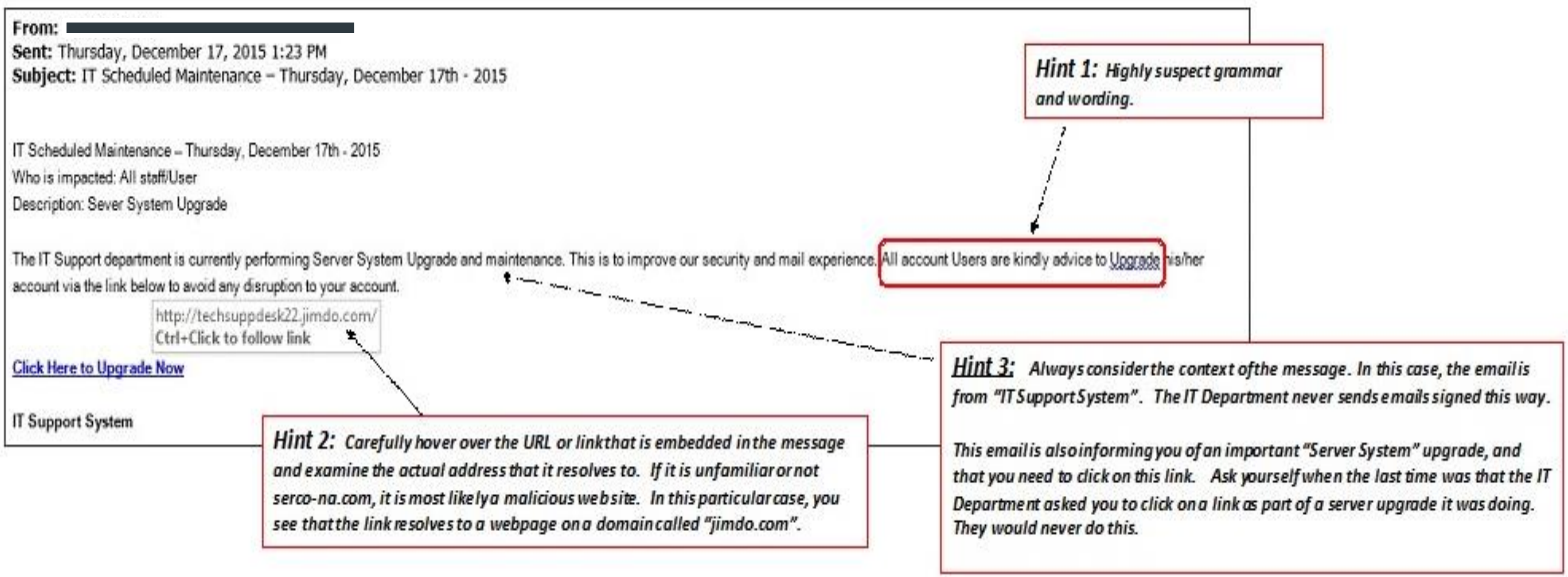
Source: "2016 Data Breach Digest" | Verizon RISK Team

Preparing An Effective Cyber Defense Plan

Why Phishing Is So Successful – A Closer Look

The level of sophistication and authenticity of phishing emails has increased dramatically over the past 2 years, increasing the likelihood that a users will be fooled and click on something they shouldn't

The email below claims to be from the IT Department and asks you to click on a link to log on to an internal web page – *What's Wrong With This Email?*



From: [redacted]
Sent: Thursday, December 17, 2015 1:23 PM
Subject: IT Scheduled Maintenance – Thursday, December 17th - 2015

IT Scheduled Maintenance – Thursday, December 17th - 2015
Who is impacted: All staff/User
Description: Sever System Upgrade

The IT Support department is currently performing Server System Upgrade and maintenance. This is to improve our security and mail experience. All account Users are kindly advice to Upgrade his/her account via the link below to avoid any disruption to your account.

http://techsuppdesk22.jimdo.com/
Ctrl+Click to follow link

Click Here to Upgrade Now

IT Support System

Hint 1: Highly suspect grammar and wording.

Hint 2: Carefully hover over the URL or link that is embedded in the message and examine the actual address that it resolves to. If it is unfamiliar or not serco-na.com, it is most likely a malicious website. In this particular case, you see that the link resolves to a webpage on a domain called "jimdo.com".

Hint 3: Always consider the context of the message. In this case, the email is from "IT Support System". The IT Department never sends emails signed this way.

This email is also informing you of an important "Server System" upgrade, and that you need to click on this link. Ask yourself when the last time was that the IT Department asked you to click on a link as part of a server upgrade it was doing. They would never do this.

Preparing An Effective Cyber Defense Plan

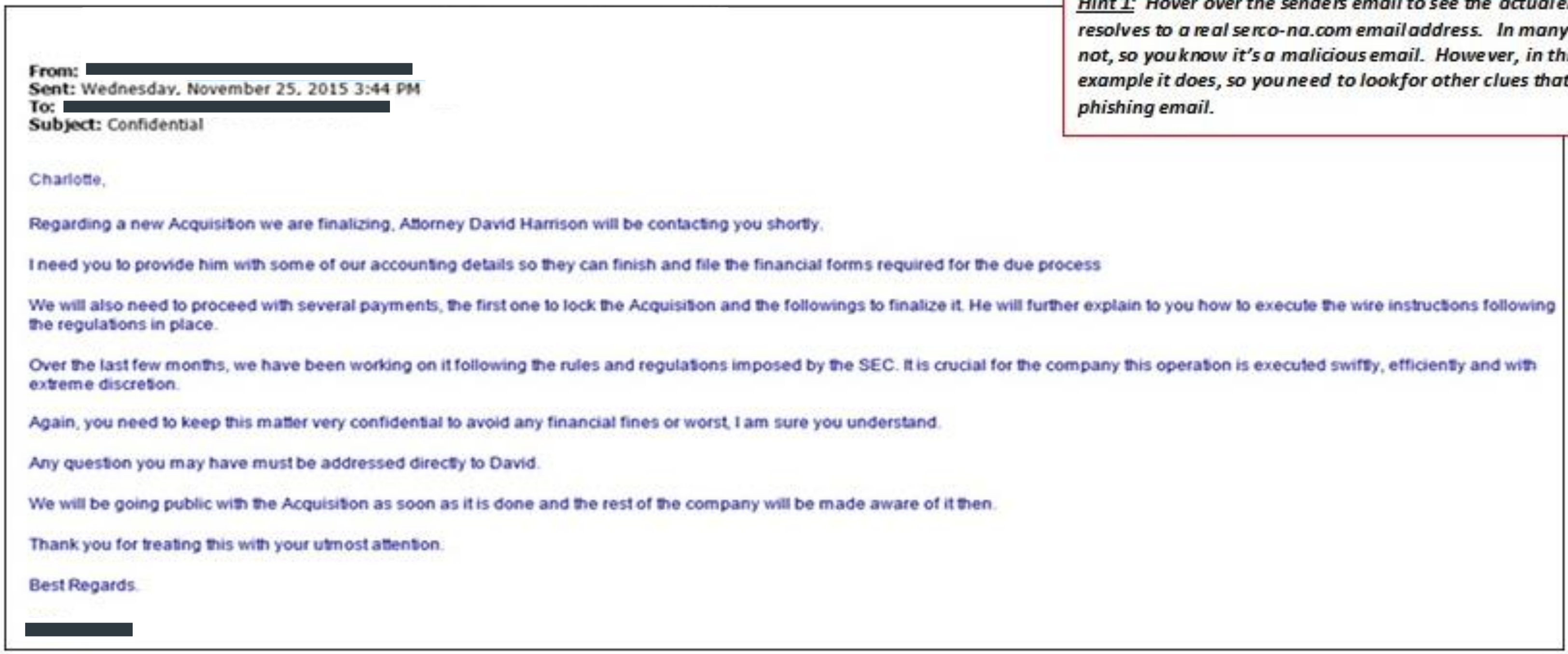
Why Phishing Is So Successful – A Closer Look

Here’s anther example of a sophisticated phishing email that was attempting to gather information that would allow a criminal attacker to steal money from the company

The below email appears to use a genuine sender email address, and the message content reads as genuine – how would you know this is phishing, what should you do?

- As with the previous example, consider the context - Would your company typically conduct business this way?
- In cases like this, it’s best to always speak to the sender directly to confirm this is genuine

Hint 1: *Hover over the senders email to see the actual email address resolves to a real serco-na.com email address. In many cases, it will not, so you know it’s a malicious email. However, in this sophisticated example it does, so you need to look for other clues that this might be a phishing email.*



From: [redacted]
Sent: Wednesday, November 25, 2015 3:44 PM
To: [redacted]
Subject: Confidential

Charlotte,

Regarding a new Acquisition we are finalizing, Attorney David Harrison will be contacting you shortly.

I need you to provide him with some of our accounting details so they can finish and file the financial forms required for the due process

We will also need to proceed with several payments, the first one to lock the Acquisition and the followings to finalize it. He will further explain to you how to execute the wire instructions following the regulations in place.

Over the last few months, we have been working on it following the rules and regulations imposed by the SEC. It is crucial for the company this operation is executed swiftly, efficiently and with extreme discretion.

Again, you need to keep this matter very confidential to avoid any financial fines or worst, I am sure you understand.

Any question you may have must be addressed directly to David.

We will be going public with the Acquisition as soon as it is done and the rest of the company will be made aware of it then.

Thank you for treating this with your utmost attention.

Best Regards.

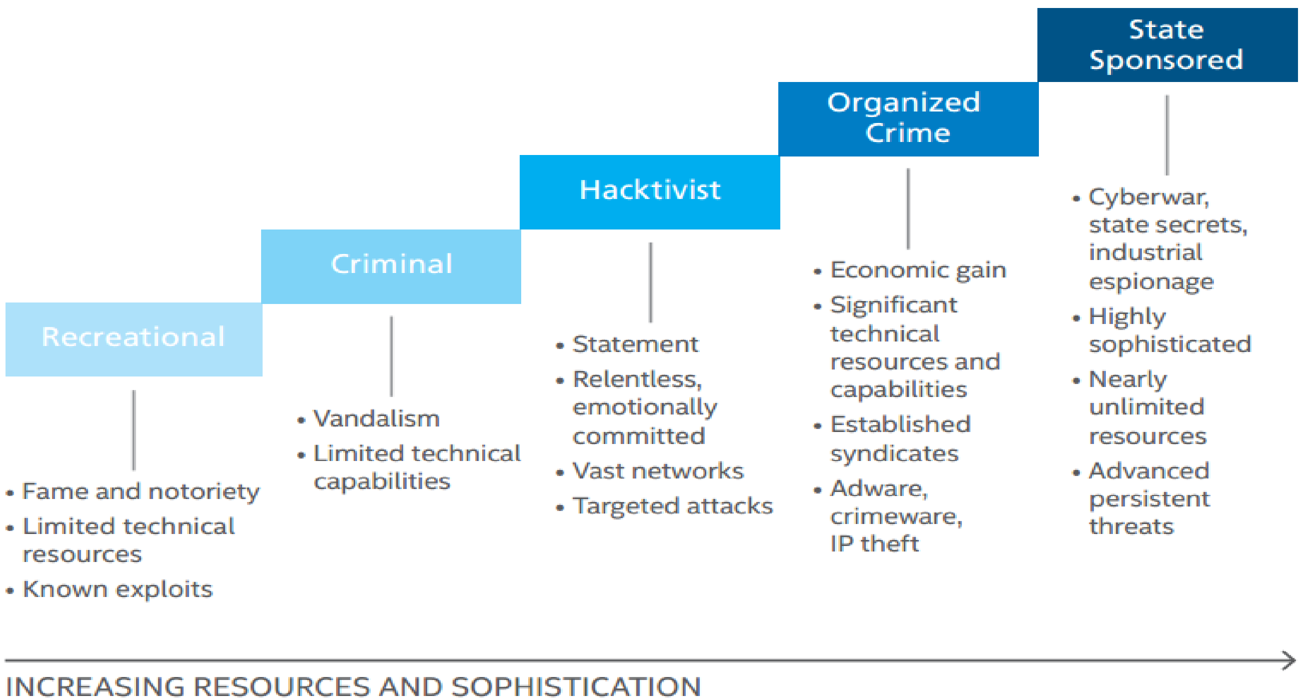
[redacted]

Preparing An Effective Cyber Defense Plan

Know Your Enemy

Understanding the different threat actors and their tactics will help you understand your particular risks and vulnerabilities that you need to protect against

Changing Attacker Profiles



Recreational

- Fame and notoriety
- Limited technical resources
- Known exploits

Criminal

- Vandalism
- Limited technical capabilities

Hacktivist

- Statement
- Relentless, emotionally committed
- Vast networks
- Targeted attacks

Organized Crime

- Economic gain
- Significant technical resources and capabilities
- Established syndicates
- Adware, crimeware, IP theft

State Sponsored

- Cyberwar, state secrets, industrial espionage
- Highly sophisticated
- Nearly unlimited resources
- Advanced persistent threats

INCREASING RESOURCES AND SOPHISTICATION

Source: "McAfee Labs Threat Report, August 2015 | McAfee

Detection & Response

How Do You Know If You've Been Hacked?

Depending on the method used, or the tools you have in place, you may or may not know if you've been attacked

- In almost all cases, by the time you find out the damage has already been done

Criminal Attacks (Individual or Organized)

- In most cases of criminal cyber attacks, victims know right away or soon after that they've been attacked
  - Example: Ransomware will immediately encrypt your endpoint or data and provide you with instructions on how to obtain the key

State Sponsored Attacks

- The objective of State Sponsored attacks is to obtain state secrets or conduct industrial espionage
- State Sponsored attacks rely on stealth for success
  - They don't want you to know they are there so they can remain embedded and steal data undetected

Detection & Response
How Do You Know If You've Been Hacked?

Quick detection, containment, and response are all critical to minimizing the impact of an attack

Detection focuses on how quickly you can detect a threat on your network

- "Dwell Time". This includes the time from when someone clicks (you are compromised) until the time the malware is no longer effective, whether that be by blocking command and control so it cannot communicate or by taking the compromised box(es) off the network.[1]
- Ensure that you are logging security, system, and application events at an appropriate level
- Consider Security Information and Event Management (SIEM) tools to help provide real time analysis on security events

Containment focuses on keeping the threat from moving laterally across your network to infect/compromise other devices

- More sophisticated threats, like some of the recent Ransomware attacks, have the ability to quickly move laterally across your network to inflict maximum damage before you are able to respond
- Remove the compromised device from the network
- Network enclaves can help contain a treat from spreading

Response focuses on how quickly you are able to react once you know you've been attacked

- Being able to mobilize and remove the treat from your network is key to minimizing the damage
- Have a documented process with steps clearly defined to orchestrate your response if an attack occurs

[1] Source: "Detect, Contain, and Control Cyberthreats" | SANS Institute, InfoSec Reading Room

Detection & Response

How Do You Know If You've Been Hacked?

The challenge facing most companies is to know how much to invest in your capabilities to detect, contain, and respond to cyber threats

- Investment = People *(properly trained cyber professionals)* + Tools
- Companies will typically base this decision on their size, sensitivity of the information they are protecting as well as the impact of the potential damage that a cyber attack and loss of data/information will have

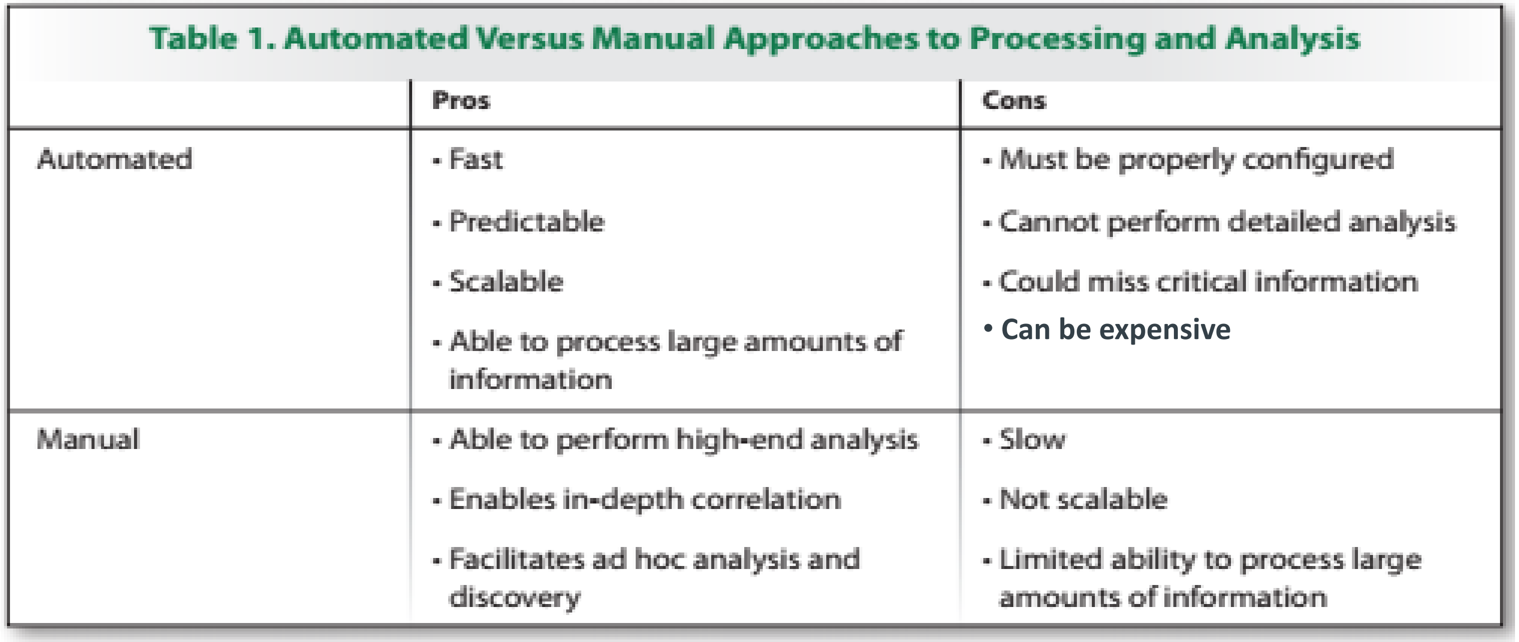


Table 1. Automated Versus Manual Approaches to Processing and Analysis

	Pros	Cons
Automated	• Fast • Predictable • Scalable • Able to process large amounts of information	• Must be properly configured • Cannot perform detailed analysis • Could miss critical information • **Can be expensive**
Manual	• Able to perform high-end analysis • Enables in-depth correlation • Facilitates ad hoc analysis and discovery	• Slow • Not scalable • Limited ability to process large amounts of information

Source: "Detect, Contain, and Control Cyberthreats" | SANS Institute, InfoSec Reading Room

Remediation

Once They're In, How Do You Get Them Out?

Remediation efforts necessary to remove a cyber threat from your network can vary greatly from Low Impact/Low Cost to Extreme impact/Extreme cost

The level of remediation will have a direct correlation to the sophistication of both the attack and the attacker

- Less sophisticated or lower impact attacks can often be remediated by quickly isolating a device(s) from the network and cleaning off the virus or malware
- The more sophisticated and higher impact attacks, such as those from Organized Crime or State Sponsored organizations, will generally require a more extensive response

Organized Crime & State Sponsored Attacks

- Remediating these types of attacks often require the professional services of a Security Remediation Firm
- These firms are engaged when you are the most vulnerable and are able to command very high fees, usually on a T & M basis
  - It's not uncommon for these firms to charge up to $400/hour
  - Cybersecurity insurance policies are becoming more and more popular as the impact to remediate advanced attacks continues to rise

How Do You Know Your Done
When Do You Have Enough Protection

The short answer is you are *never* done and *never* totally protected

- The challenge is to stay one step ahead of the attackers, but the reality is you may struggle to keep up with them
- Your Cyber Defense Plan will always be changing and evolving to keep step with the changing and evolving threats
- Prioritize cyber security from the top down to ensure that the focus does not fade over time
- Maintain a holistic Cyber Defense Plan that is multi-layered and right sized for your organization
- Approach training and awareness from the bottom up to ensure that everyone is taking cyber security seriously and remains vigilant
- Know when to get outside help – a good cyber security defense and response plan can be complicated and intimidating

Thank You