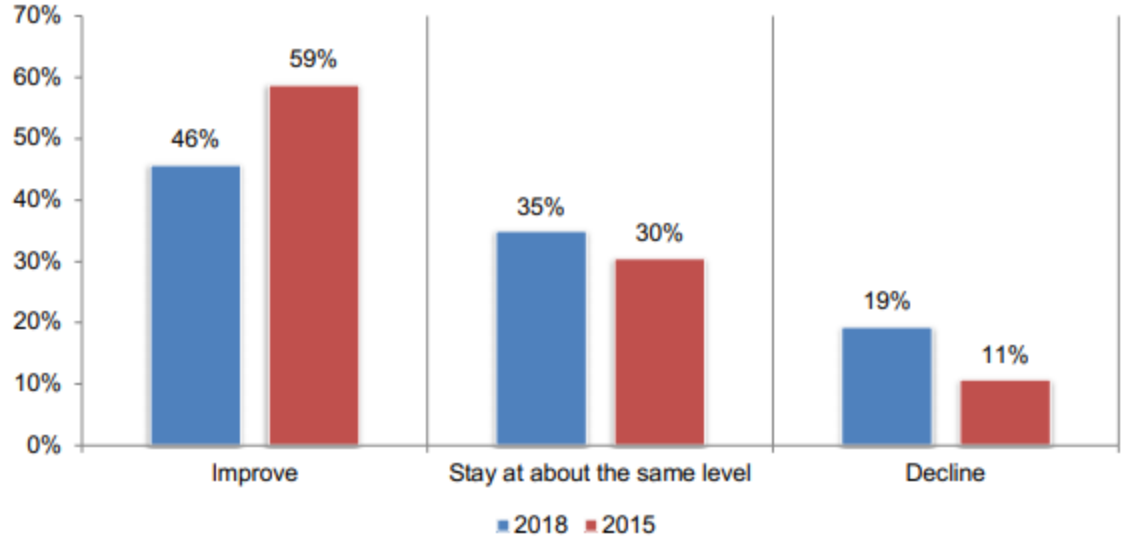
Top 3 “Priorities” on our mind… Today? This week? This month?

Ponemon Institute: Organization's Security Posture 2018 vs. 2015

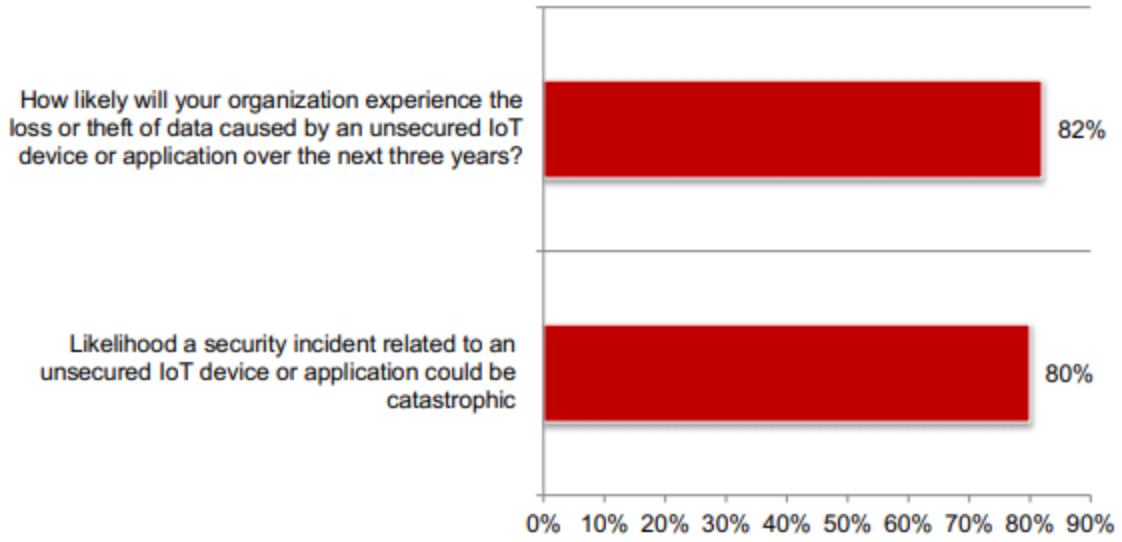
Figure 1. Will your organization's cybersecurity posture improve in the next three years?



Ponemon Institute: Organization's Security Posture IoT Devices

Respondents predict that a data breach caused by an unsecured IoT device is likely. Figure 9 reveals that 82% of respondents say it is very likely, likely and somewhat likely that their organization will experience a data breach caused by an unsecured IoT device in the workplace; 80% believe this type of data breach could be catastrophic.

Figure 9. An IoT data breach is likely and it could be catastrophic
Very likely, Likely and Somewhat likely responses combined



Ponemon Institute: Organization's Security Posture MSSP

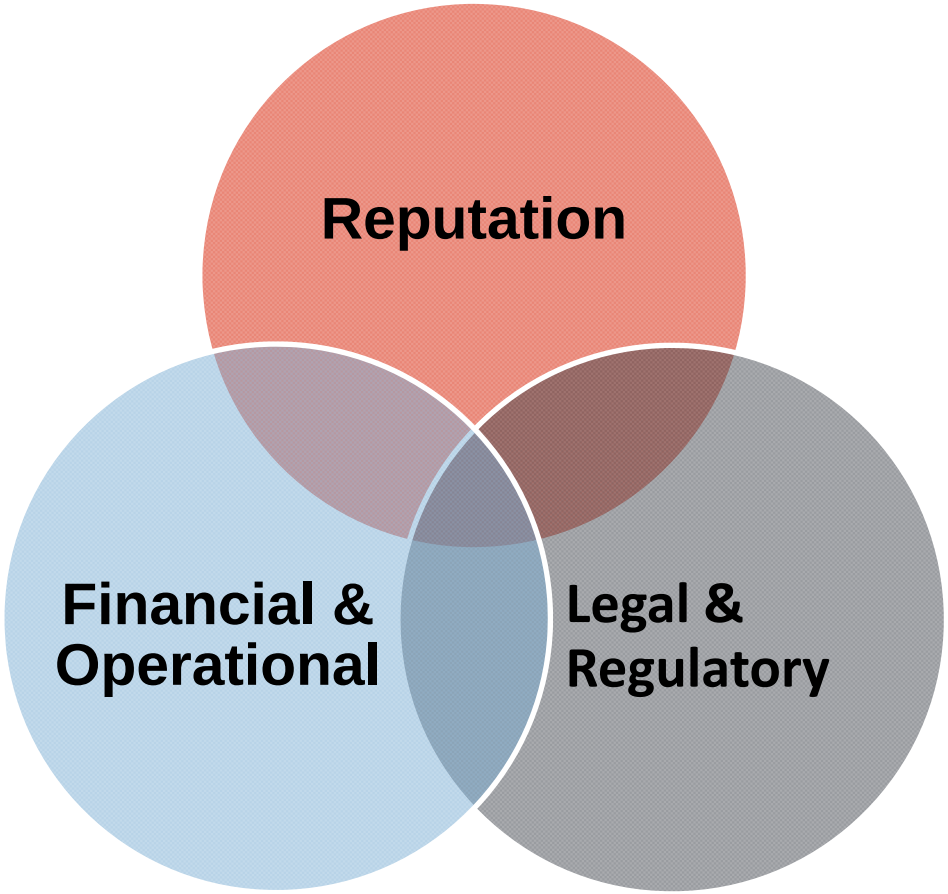
Table 6. Megatrends: Organizational risks			
Organizational factors	Today	Future	Difference
Integration of third parties into internal networks and applications	43%	59%	16%
Inability to recruit and retain qualified ITS personnel	48%	62%	13%

More companies will be hiring managed security services (MSS) to address the lack of skilled in-house staff. As discussed previously, more companies are predicted to engage MSS providers. As shown in Figure 8, almost all companies represented in this research believe these services will become an important part of the overall IT security strategy (80% of respondents).

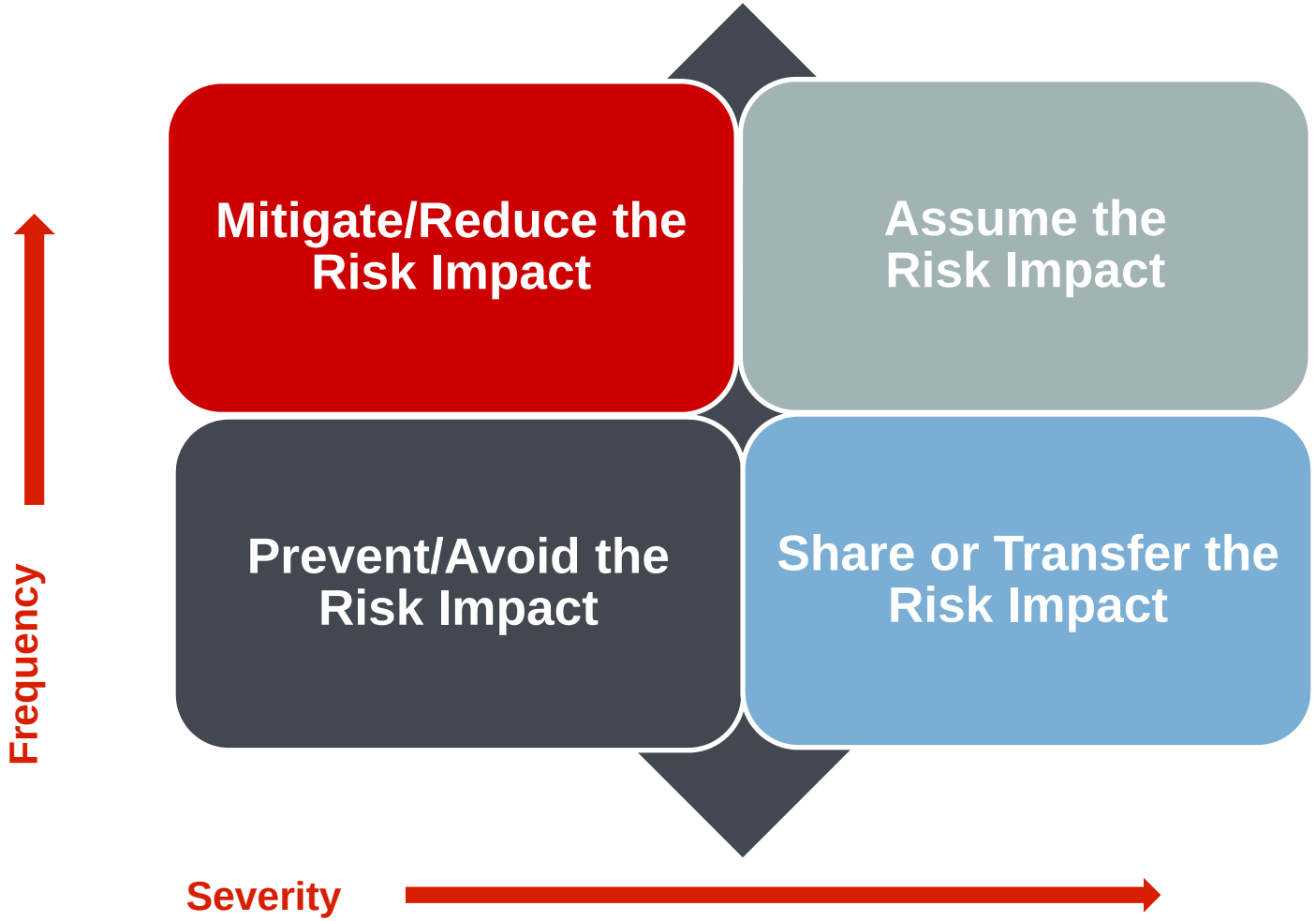
Figure 8. Predictions about the importance of MSS
Essential, Very important and Important responses combined

Risk Management Fundamentals

How Risks Impact the Business



Frequency & Severity Risk Action Paths

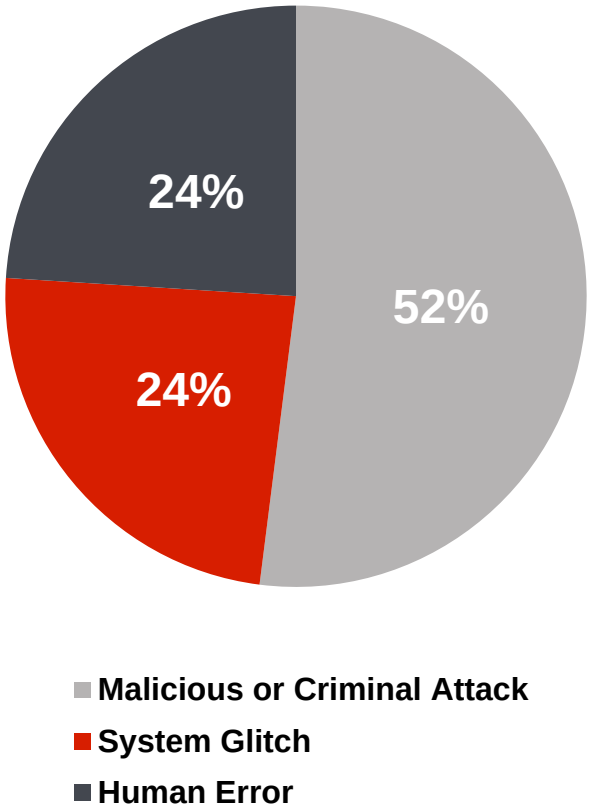


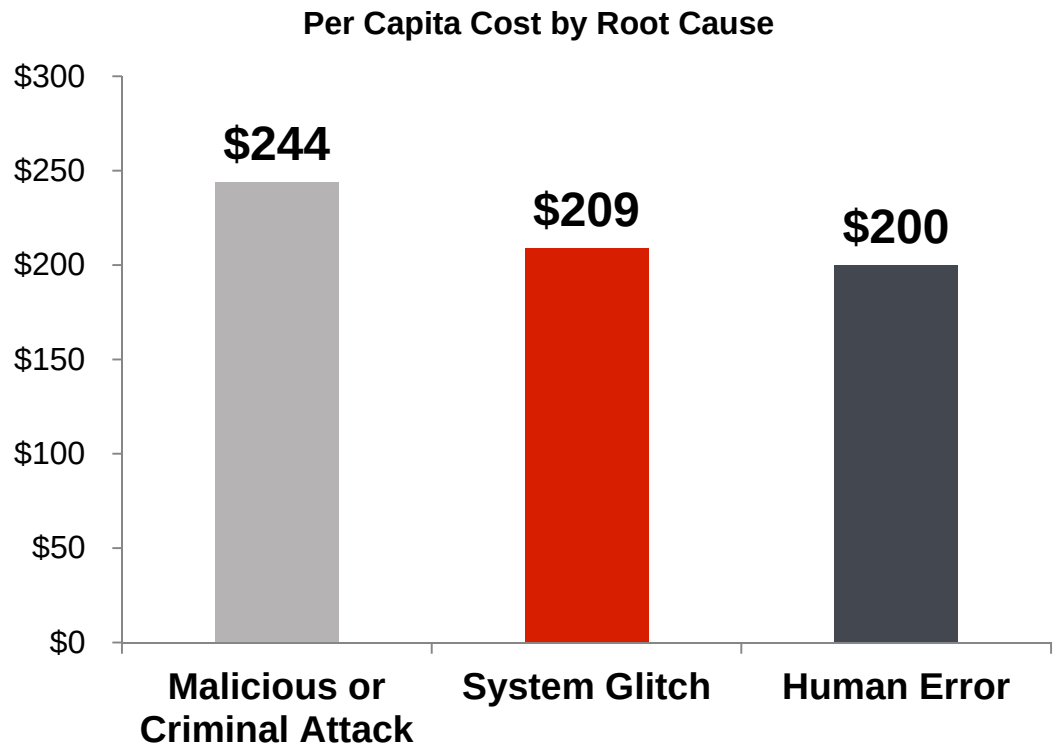
Cyber Security

Impacts and Trends

Impacts & Trends

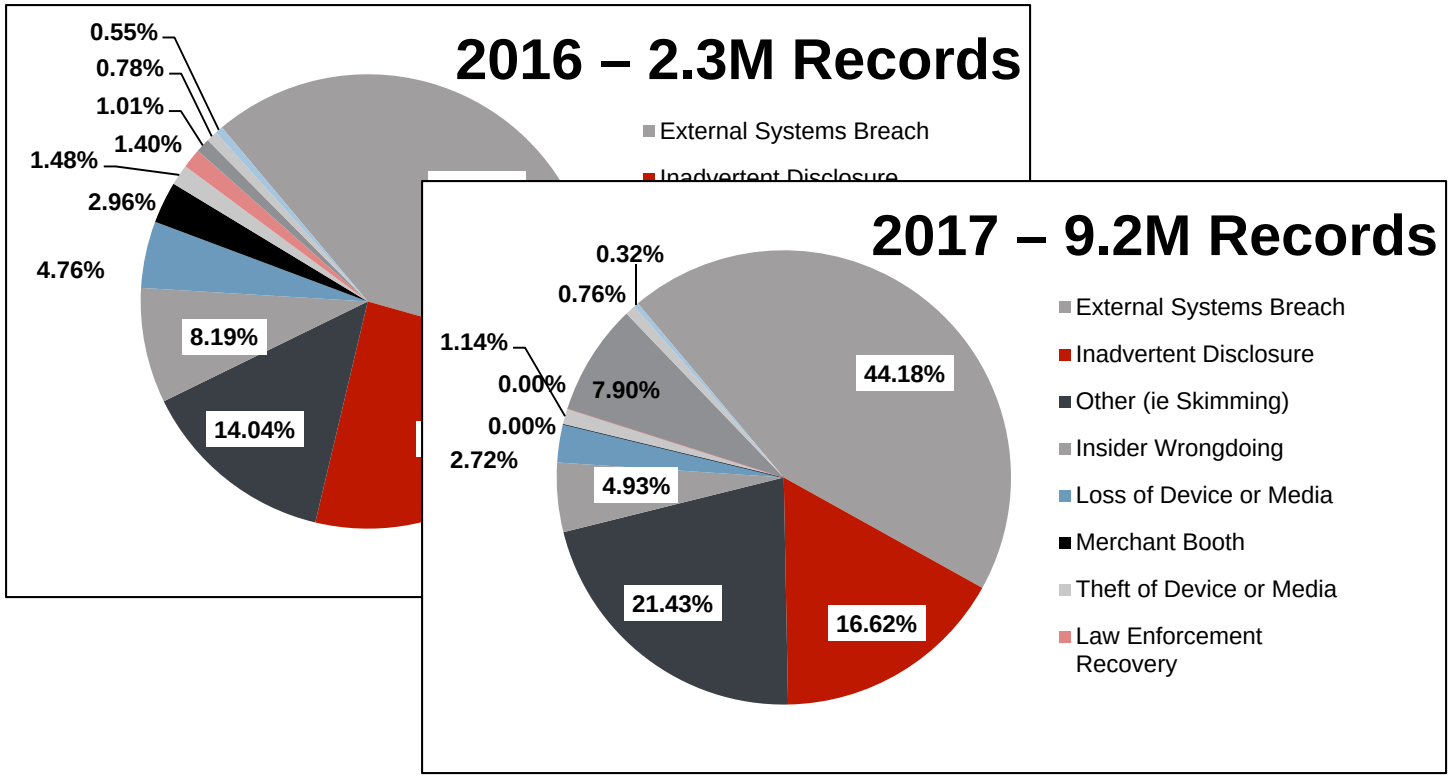
Malicious or Criminal Attacker	System Glitch	Human Error





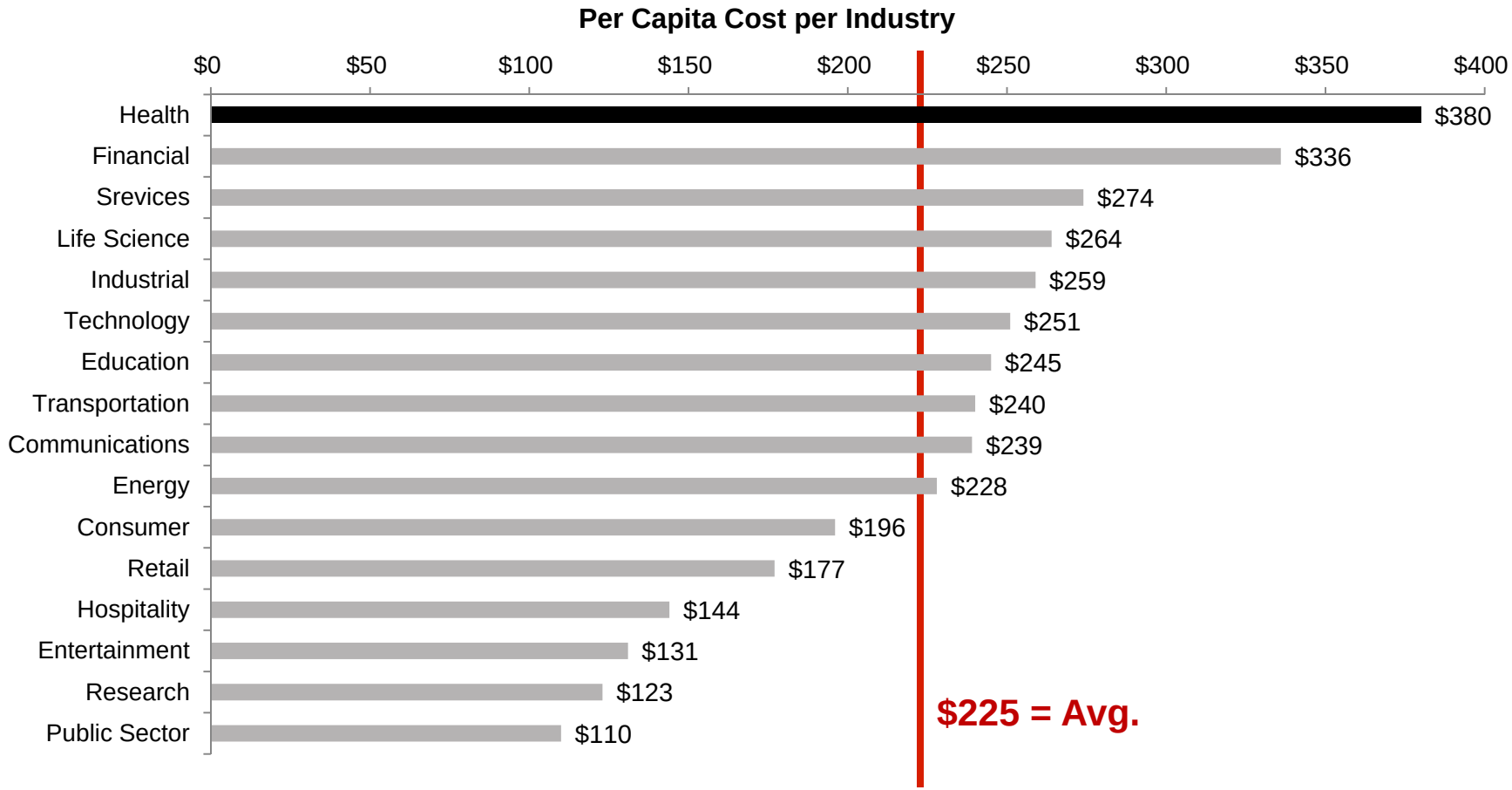
Ponemon Institute Cost of Breach Study - U.S.

Data Breach Statistics - NYS AG Schneiderman



https://ag.ny.gov/press-release/ag-schneiderman-announces-record-number-data-breach-notices-2016

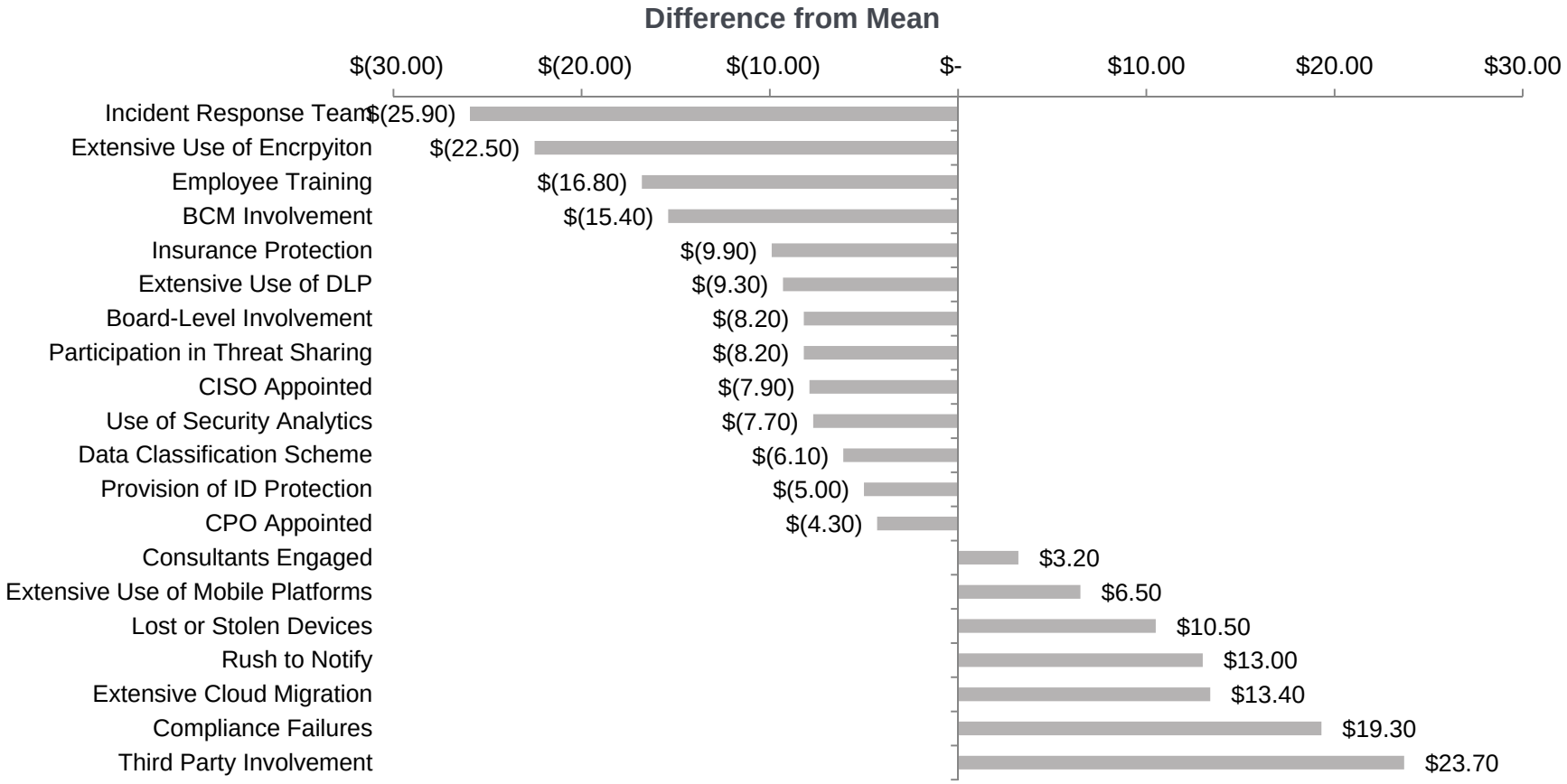
Cost of Data Breach Study (Ponemon Institute) – June 2017 Report



Ponemon Institute Cost of Breach Study - U.S.

Data Breach Cost Drivers - Ponemon Institute 2016 Report

Impact of 20 Factors on the per capita cost of a data breach



Ponemon Institute Cost of Breach Study - U.S.

Cyber Security

Criminal Minds & Human Error

Human and Technology against the World of Risk

Technological defense mechanisms and training for humans are the defense against the world of risk.

World of Risk

Hacking is unauthorized intrusion into a computer or a network.

- There are two types: good (white hat hackers) and bad (black hat hackers).
- Hackers attack our security countermeasures to achieve their goals.
- Hacking's goals can be politically/financially motivated, corporate espionage, terrorist, revenge, or status based.

Employee theft subverts security countermeasures for the same goals as the hackers.

Theft by real thieves for the same goals as the hackers.

Employees and decision makers lack security knowledge, making it easier for the world of risk to achieve their goal. It is my hope that they do not knock on your door.

http://searchsecurity.techtarget.com/definition/vulnerability-scanning

Criminal Methods

Brute Force – Little thought. Throw stuff at the wall and see what sticks.

Sophisticated – Acquire information about the target and attack with purpose and direction. The more sophisticated it is, the less likely you will know it even happened. If you are not looking you will never see it coming until it is too late.

This years primary attack vector

- **Dark Web**
- **Pineapple Attack**
- **Metadata & Your Fingerprint**
- **Bypassing the Firewall**
- **Phishing & SMiShing**
- **Spear Phishing**
- **Social Engineering**

http://searchsecurity.techtarget.com/definition/vulnerability-scanning

Primary Attack Vector - 2018

- E-mails with links and attachments quarantined and released by staff
- E-mails received and opened with word or pdf attachments and the staff had to enable macros. They then forwarded the message to others to try and open it as well.
- The attachments are downloaded from various file sharing sites.
- The macro then downloads other files to infect initial system.
- Those files then run as the current user.
- If that user is a local admin then the infection gets the ability to create services and replace files.
- If that user is a local admin on another computer or a domain admin then the entire network is at risk and under attack.

Welcome to the Dark Web

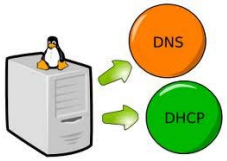
- Designed to be untraceable by the US military to communicate with intelligence assets.
- Uses Tor, Onion Routers, Hidden websites
- You need a special Tor browser like TAILS to access it
- Search engines do not index it.
- Darknet markets operate within it selling drugs, body parts, weapons, PHI, Credit Cards, organizing hits to kill people and it is where hackers work and live.
- Multiple currencies are used including Bitcoins to pay for services rendered.
- If you enter into this world prepare to be infected.
- This is the world that is hired to attack you, used to attack you, and profits from the attack upon you.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

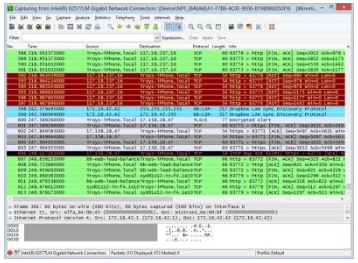
Pineapple Attack

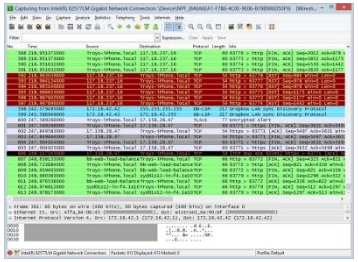
Can occur at hotels, Starbucks, library…anywhere WIFI is available.

- You unknowingly connect to the attacker's WIFI instead of the real WIFI. Now you're in trouble.



- The attacker monitors your traffic, sees what you type and controls where you go.





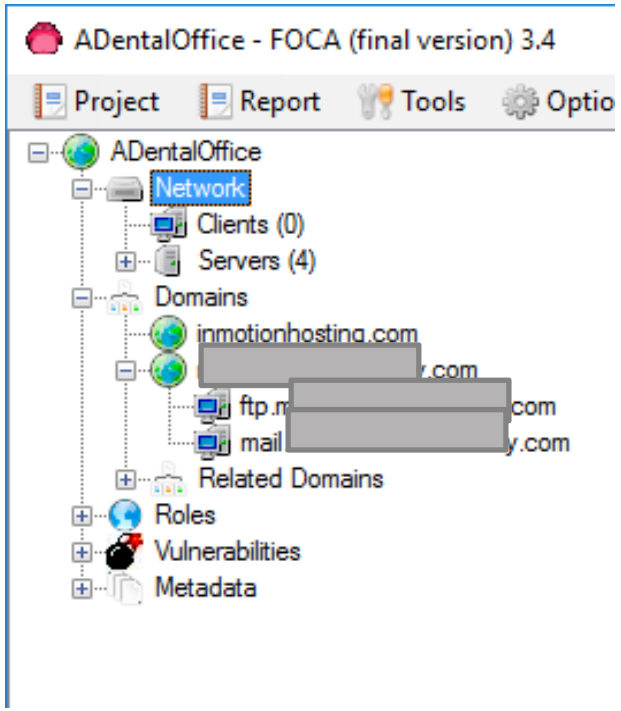
- The attacker can spin up fake websites to steal your password and access your account(s). Before you know what is happening you are in a world of hurt.

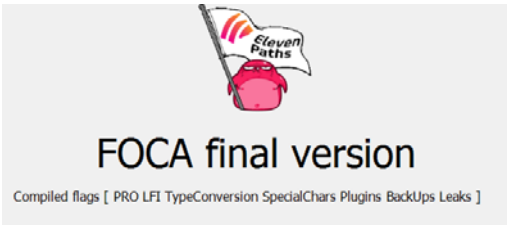
https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Meta-Data & your Fingerprint

Foca Pro is a free tool. It can exploit your internet finger print.

- It finds and grabs the finger print you have left on the internet.
- It identifies your computers, systems, users, operating systems, and applications.
- It allows hackers to use this information to target your business with minimal effort.
- Within seconds of opening this tool the hacker can determine the hosting company, and the mail, DNS and FTP server as well as other companies hosted on the same system and their names.
- The hacker can attack this client and all other clients on the server using email based methods.
- Just like X-Rays help you do your job, FOCA Pro and tools like it help hackers attack you.



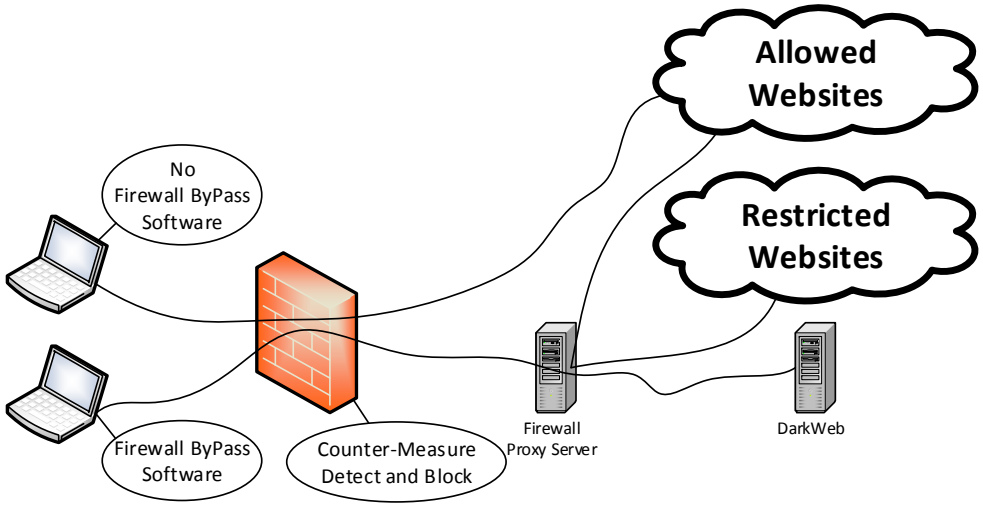


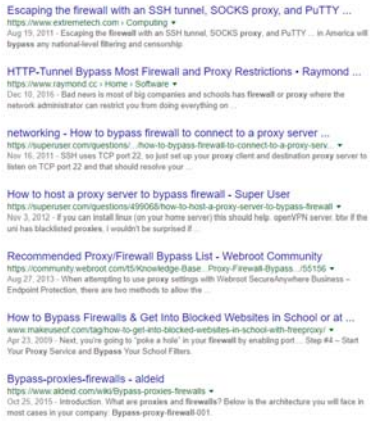
https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Bypassing the Firewall

- SSH Tunnel, SOCKS Proxy, Proxy Server, Putty are great tools for the bad guys.
- **Hackers want to get in, achieve their goal on your network, and get out.**
- Hackers have to actively circumvent your security measures.
- Hackers write code and they have added this technology into their applications to allow them to succeed at their goals. (Measures / Countermeasures)

The first goal is to stop hackers from getting in. If they do manage to infiltrate your system, find them as soon as possible and stop a secondary attack.




Escaping the firewall with an SSH tunnel, SOCKS proxy, and PuTTY ...
https://www.extremetech.com › Computing
Aug 19, 2011 - Escaping the firewall with an SSH tunnel, SOCKS proxy, and PuTTY ... in America will bypass any national-level filtering and censorship.

HTTP-Tunnel Bypass Most Firewall and Proxy Restrictions - Raymond ...
https://www.raymond.cc › Home › Software
Dec 10, 2016 - Bad news is most of big companies and schools has firewall or proxy where the network administrator can restrict you from doing everything on ...

networking - How to bypass firewall to connect to a proxy server ...
https://superuser.com/questions/.../how-to-bypass-firewall-to-connect-to-a-proxy-serv...
Nov 16, 2011 - SSH uses TCP port 22, so just set up your proxy client and destination proxy server to listen on TCP port 22 and that should resolve your ...

How to host a proxy server to bypass firewall - Super User
https://superuser.com/questions/499068/how-to-host-a-proxy-server-to-bypass-firewall
Nov 3, 2012 - If you can install linux (on your home server) this should help. openVPN server. btw if the uni has blacklisted proxies, I wouldn't be surprised if ...

Recommended Proxy/Firewall Bypass List - Webroot Community
https://community.webroot.com/t5/Knowledge-Base...Proxy-Firewall-Bypass.../55156
Aug 27, 2013 - When attempting to use proxy settings with Webroot SecureAnywhere Business – Endpoint Protection, there are two methods to allow the ...

How to Bypass Firewalls & Get Into Blocked Websites in School or at ...
www.makeuseof.com/tag/how-to-get-into-blocked-websites-in-school-with-freeproxy/
Apr 23, 2009 - Next, you're going to "poke a hole" in your firewall by enabling port ... Step #4 – Start Your Proxy Service and Bypass Your School Filters.

Bypass-proxies-firewalls - aldeid
https://www.aldeid.com/wiki/Bypass-proxies-firewalls
Oct 26, 2015 - Introduction. What are proxies and firewalls? Below is the architecture you will face in most cases in your company. Bypass-proxy-firewall-001.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Phishing (Social Engineering)

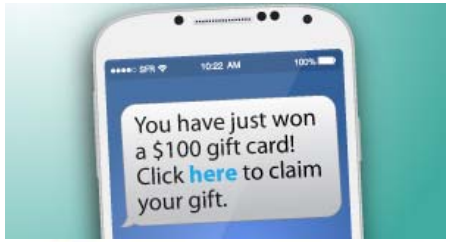
Phishing is the attempt to obtain sensitive information and achieve the hacker's goal.

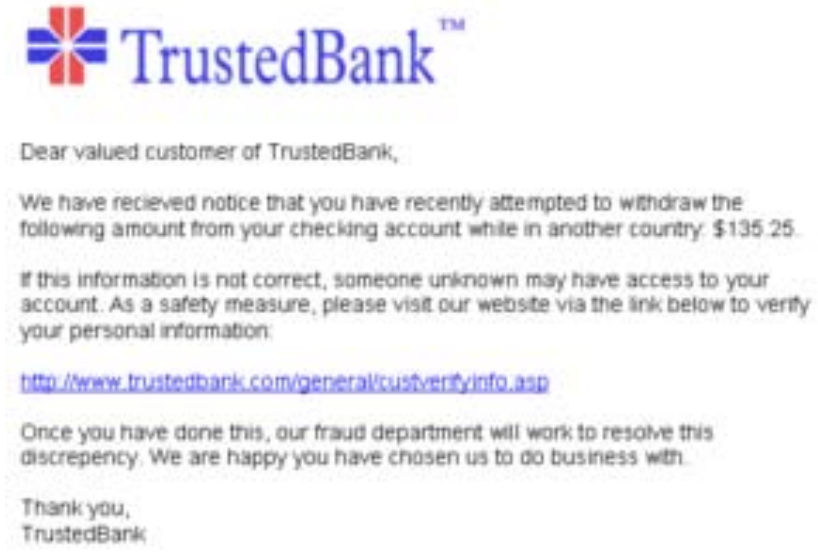
If they are sophisticated they want to see what emails are good and what emails are bad. They want to move on to spear fishing.

If they are not sophisticated they just want to find anyone that will take the bait by disguising themselves as a trustworthy entity.

Phishing is typically carried out by email spoofing or instant messaging. (**SMiShing – SMS Phishing**)

- It can direct you to a fake website with the same look and feel as the legitimate one. This is known as a **pineapple attack**.
- It can be used to infect your system, gain control, and achieve the hacker's goal.




TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

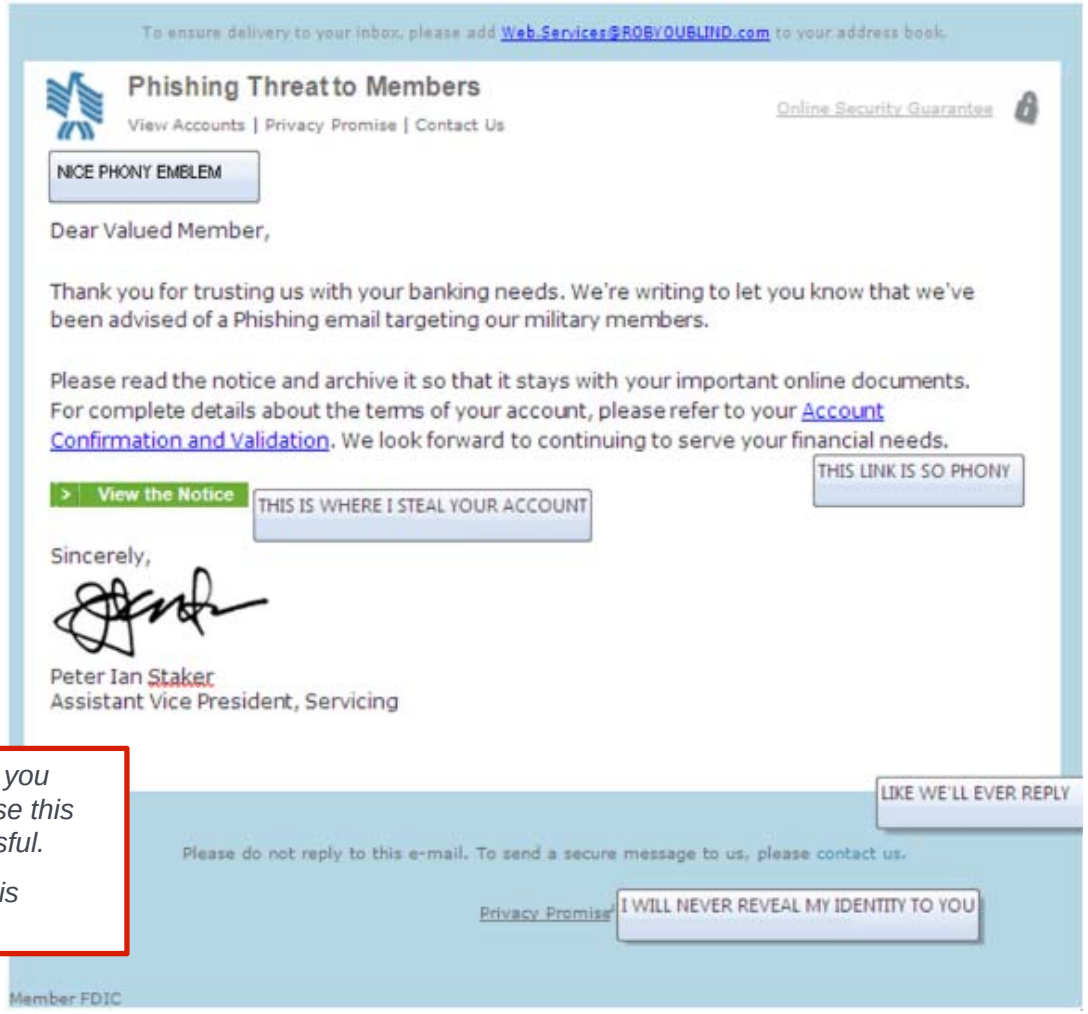
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Spear Phishing (Social Engineering)

- **Spear phishing is targeted and sophisticated.**
- **It requires information. The more the hacker has the more successful the attack will be.**
- **Media: Email, mail and phone (A good campaign uses all three and ties it together.)**
  - Yes, I said phone. An Astar phone system with SIP and recording of the automated attendant fools you and puts you, your business and your clients at risk.
- **Social engineer wants you to believe they are credible and real to gain your trust.**
- **Consider a way to verify. The more information you expose, the more information they have to use on their next attack gaining your trust.**



Example: If a hacker discovers where you do banking, then you have a target painted on your back. The hacker can now use this information to send targeted message and be more successful.

So, a physical mailing list, phone numbers and/or email list is money in the bank to criminal minds.

http://searchsecurity.techtarget.com/definition/vulnerability-scanning

Ransomware (Crypto & WannaCry)

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

- Why should you care about this one? Because HHS has said that any business hit by Crypto and Ransomware is consider to have had a breach event.
- Their strict interpretation of the law is that you have lost control of your medical records and therefore it is a breach of ePHI.

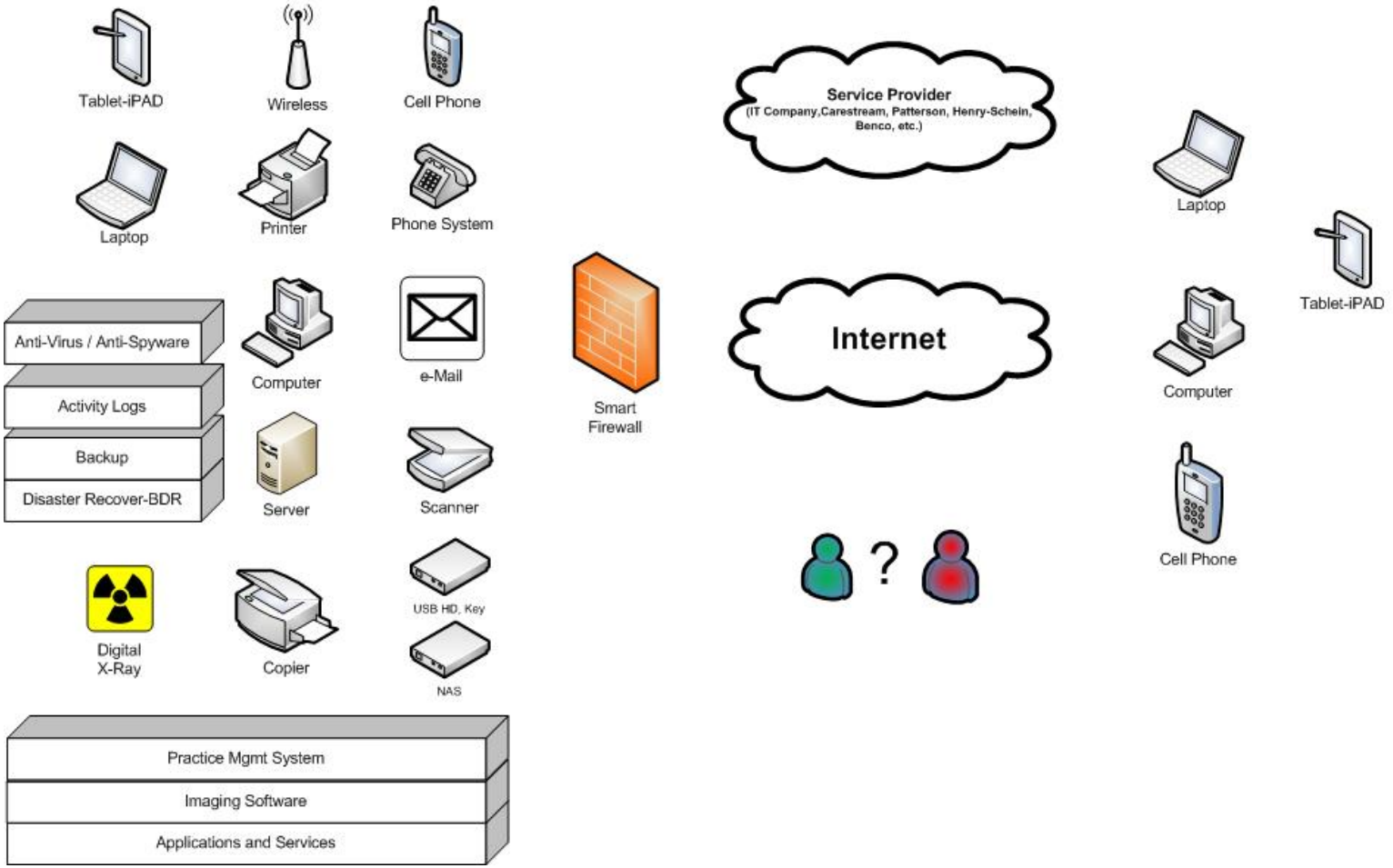
Great reason for MSSP with a system that protects your business from ransomware's success. This is not a do it yourself solution. You need a skilled professional with a solution that protects you, your business and your clients. If you don't have one, get one.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Cyber & Privacy Risk

“Basics of IT Defenses”

Know Your System / Know Your People

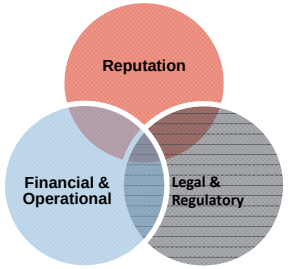


Risk Management

Manage Risk with Control

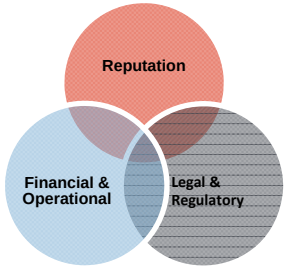
Define and follow your policies and procedures to manage business risk

1. **Address the Attack Vectors** (Hackers and others look for holes / Fill the holes)
2. **Address Breach Vectors** (They exploit the hole / Fill the holes)
3. **Address Fine Vectors** (They look at what you have done and not done to assess the fine / Fill the holes)



Physical Control

Risk Management



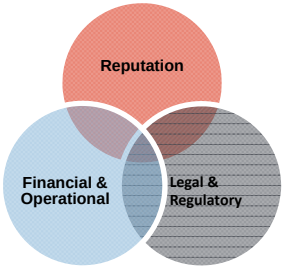
Manage Risk with Control

Define and follow your policies and procedures to manage risk

1. **Address Attack Vectors** (Hackers and others look for holes / Fill the holes)
2. **Address Breach Vectors** (They exploit the hole / Fill the holes)
3. **Address Fine Vectors** (They look at what you have done and not done to assess the fine / Fill the holes)

Attack Vectors	Breach Vectors	Fine Vectors
People	People	Breach Event
Internet Apps	Unvetted Internet Apps	No HIPAA Manual
Web Commutations	Web Communications	(Privacy/Security)
E-Mail	E-Mail	No Training Evidence
BYOD	BYOD	No Evidence Manual Followed
Remote Access	Remote Access	No Risk Assessment
IoT	IoT	No Notice of Privacy Practice
	Media Disposal	
	Fax	
	Voice Mail	

Risk Management



Control

IN

OUT

Policies & Procedures

IN

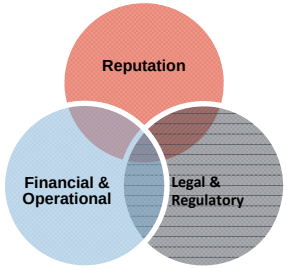
YOUR BUSINESS

OUT

Internet

Monitor, Review & Report

Risk Management – Train Your Staff



What is the primary purpose?

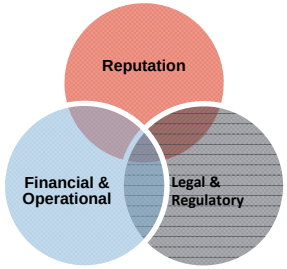
- People are your primary attack vector and breach vector
- Reduce the risk your business faces by connecting to the internet.

How does this apply?

- Follow processes and procedures they remember
- Answer phones and talk with people (Good and Bad)
- Use your computer system
- Use the internet on your computers to support the business and personal activities
- Use their devices while they are in your office
- They may even connect their phone to your computer.
- Use email to communicate
- Notice system performance issues
- Report things they don't think are right
- Ask for guidance before and after a problem occurs

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Training



Top training assumptions that put your business at risk

- Data breaches occur through the internet
- I trained them once they should know it
- My system will protect me

What do I do?

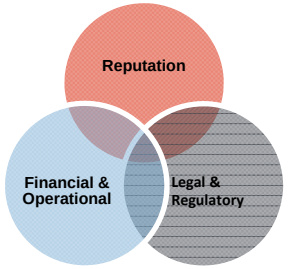
- Perform training, remind and control
- Prepare your people for cyber risks
- Prepare your people for social engineering attacks (Phone, Fax and Internet).
- Prepare your people for physical risk

Why?

- People are your first line of defense.
- People are your first attack vector for your business.
- Minimize risk to you and your business.

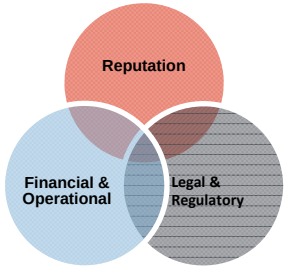
https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Information Technology & Risk Management



- Firewalls
- Anti-virus
- Patching
- Event Monitoring
- Backup
- Disaster Recovery
- Intrusion Detection Systems
- Virtual Private Network
- Vulnerability Scanning
- Encryption

Firewalls (NGFW)



What is it?

A firewall is a network security system designed to prevent unauthorized access to or from a private network

What is their primary purpose?

- **Reduce Risk** that your business faces by connecting to the internet.

A poorly configured firewall, *that is not monitored and does not have reporting*, does your business no good.

How do they work?

- **Separate** – Your computers from the world
- **Route** – Connect your computers to the world
- **Restrict** – Control what communications occur with the world
- **Monitor** – Look at what communications are occurring between your computers and the world.
- **Protect** – Identify and stop risky communications (Viruses, Spyware, intrusion, GeO Graphical, Known Bad Servers)
- **Report** – Log and generate reports on a periodic basis for risk management.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Firewalls

Top Firewall Assumptions that put your business at Risk:

- All Firewalls are the same.
- All Firewalls work the same.
- I have a firewall, therefore, my network is safe.
- A firewall that never has to be changed is a good firewall.
- My firewall stops the bad guys from getting in to my network.
- My IT Guy has me covered.
- This is too complicated for me to understand.

What do I do?

- Understand what security your firewall provides your business.
- Implement the firewall based on risk management
- Get objective evidence you are protected (Activity Report).
- Review the report with your IT Service Provider.

Why?

- Minimize Risk to you, your business, and your customers.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Firewalls

Consider This…

Indications of a poorly configured firewall and indication your network is at risk:

- ❑ You add new equipment and don't update the firewall
- ❑ You add a new e-mail service and don't update the firewall
- ❑ You put something new on your network that has to communicate with the internet and you don't update the firewall.
- ❑ This means a hacker can do the same thing to you without your knowledge.

An inadequate /poorly configured firewall does not protect you or your business.

An inadequate /poorly configured firewall does not allow you to manage risk.

https://en.wikibooks.org/wiki/Information_Security_in_Education/Network_Defenses

Anti-Virus & Anti-Spyware

What is it?

- Anti-spyware software is a type of program designed to prevent and detect software that covertly gathers user information through the user's Internet connection without his or her knowledge
- Antivirus software is a class of program designed to prevent, detect and remove infections on individual computing devices, networks and IT systems.

What is the primary purpose of them?

- Reduce the risk your business faces because it is connected to the internet
- Reduce the risk your business faces when someone inserts media into your computer network

How do they work?

- Anti-virus & Anti-Spyware software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of viruses and spyware
- Protects your devices from what it knows about but cannot handle the unknown during real-time scanning.
- Protects your devices from anything it learns about by scanning the system.
- The time between new virus signature updates is the window of opportunity for infection (Attack Vector).

http://searchsecurity.techtarget.com/definition/antivirus-software

Anti-Virus & Anti-Spyware

Top Anti-Virus & Anti-Spyware Assumptions that put your business at Risk:

- Anti-Virus and Anti-Spyware Applications are all the same (or all work the same).
- My Anti-Virus and Anti-Spyware stops the bad guys from getting into my network.
- I have Anti-Virus and Anti-Spyware. It cleans and fixes everything.
- Anti-Virus and Anti-Spyware solutions that never have to change is a good thing.
- My IT Guys have me covered.

What do I do?

- Understand what security your Anti-Virus and Anti-Spyware Application provides your business.
- Implement the Anti-Virus and Anti-Spyware based on risk management
- Get objective evidence you are protected (Activity Report).
- Review the report with your IT Service Provider until you know how to read it and ask questions.

Why?

- Minimize Risk to you and your business.

http://searchsecurity.techtarget.com/definition/antivirus-software

Anti-Virus & Anti-Spyware

Consider this…..

- Anti-Virus and Anti-Spyware software do not catch everything, all the time, ever.
- As it takes time to develop antibiotics to fight infections in humans, such is true in the computing world
- The primary infection is only the start. Viruses and Spyware are designed to penetrate, assess, exploit and break into your network. They make a hole first, and then they make it bigger.

Anti-Virus & Anti-Spyware has Vulnerability - It only protects against "known infections"

- The frequency of signature update defines when you can be infected.
- The time it takes for a signature update to cover new viruses defines your risk window.
- In 2014, a senior VP at Symantec estimated that they caught only 45% of cyberattacks.
- In 2016, McAfee says it found 4 new malware strains every second.
- In 2016, Sonicwall was seeing 1200 new versions of CryptoLocker every month.

The infection cycle lives on:

- Social Engineering to get data
- Social Engineering to get data, destroy, and get money
- Attack, get data, destroy, and get money
- Attack, get data, destroy, and get money

http://searchsecurity.techtarget.com/definition/antivirus-software

Patching

What is it?

A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually called bug fixes, and improving the usability or performance.

What is the primary purpose?

- Reduce the risk your business faces when it is connected to the internet
- Fix bugs within the applications, operating systems and devices

How does it work?

- Operating System patches are released weekly or on an event driven bases.
- Microsoft Office patches are released weekly or on an event driven bases.
- Third party applications patches are released weekly or on an event driven bases.
  - Adobe Acrobat
  - Flash
  - Java
  - Adobe Air
  - Microsoft Silverlight

http://searchsecurity.techtarget.com/definition/antivirus-software

Patching

Top patching assumptions that put your business at risk:

- I enabled Microsoft automated patching. I am covered.
- I have enabled Microsoft Office automated patching. I am covered.
- I have my staff update Acrobat, Flash and Java. I'm covered.
- This stops the bad guys from getting into my network.
- My IT guys have me covered.

What do I do?

- Understand what security patching provides your business.
- Implement patching based on risk management.
- Get objective evidence patching is occurring. (Activity Report)
- Look for systems that are having problems patching.
- Review the report with your IT service provider until you know how to read it and ask questions.

Why?

- Minimize risk to you, your business, and your Clients.
- An unpatched system is vulnerable. The patches close the door.

Event Monitoring

What is it?

Event monitoring is the process of collecting, analyzing, and signaling occurrences to subscribers such as operating system processes, active database rules as well as human operators.

What is the primary purpose?

- Reduce the risk your business faces because it is connected to the internet.
- Reduce the risk your business faces because it uses computers.

How does it work?

- The Monitoring system runs on the computers as part of the Remote Management and Monitoring (RMM) agent.
- The Monitoring system notifies your service provider when an event happens on your computers.
  - Processor utilization is high (Someone is trying to break-in)
  - Account elevation to administrative level (Someone is trying to break-in)
  - There is a hardware failure (A drive is failing or memory is failing or power supply is failing.)

http://searchsecurity.techtarget.com/definition/antivirus-software

Event Monitoring

Top event monitoring assumptions that put your business at risk

- I don't need this. My business isn't that big and the risk is low.
  - With event monitoring you can detect issues before hardware fails and detect security problems
  - How much would it cost the business to shut down for two weeks as we rebuild and recover your system?
  - Keep your business running
- My IT guys have me covered.
  - How can your IT guys have you covered if they are not looking?
  - How confident are you that you could find cancer on someone's tongue with out a biopsy?

What do I do?

- Understand what event monitoring provides your business.
- Implement event monitoring based on risk management.
- Get objective evidence event monitoring is occurring. (Activity Report)
- Look for systems that are having problems monitoring.
- Review the report with your IT service provider until you know how to read it and ask questions.

Why?

- Minimize risk to you, your business, and your customers.

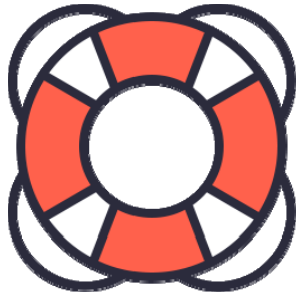
http://searchsecurity.techtarget.com/definition/antivirus-software

Backup

What is it?

Backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to ***restore*** the original after a data loss event.

What is the primary purpose?



- Reduce the risk your business faces because it is connected to the internet.
- Be able to recover corrupt files and your computer system in the event of a failure.

How does it work?

- Software is installed and configured to write your business data to external storage.
- Backups are run on a periodic basis to external storage.
- The backup frequency is the amount of transactions and data that will be lost if there is a failure occurs.
- If there is a corruption within the backup data and you have to go back to the last **GOOD** backup. You can have multiple days or hours of lost data.
- The external storage is either connected to your system or located on the internet (in the Cloud).
- The backup contains multiple copies of your business system to allow you to restore to different days because sometimes data becomes corrupt and you do not discover it until later.

http://searchsecurity.techtarget.com/definition/antivirus-software

Backup

Top backup assumptions that put your business at risk:

- I have a backup. I am covered.
- All backups are the same.
- All backups provide the same level of protection.
- When I switch IT providers I don't have to worry about the backup they were doing for me.
- My IT guys have me covered.

What do I do?

- Understand what the backup software provides your business.
- Implement backup based on risk management.
- Understand you will have data that needs to be re-entered.
- Understand you will have images that are lost.
- Get objective evidence backups are monitored and occurring (Activity Report).
- Get objective evidence the backup problems are resolved.
- Review the report with your IT service provider until you know how to read it and ask questions.
- Perform a test restore of some or part of your data on a periodic basis.

Why?

- Failures, mistakes, and malicious activities happen and you need a way to recover.
- Minimize data loss risk to you, your business, and your customers.

http://searchsecurity.techtarget.com/definition/antivirus-software

Disaster Recovery

What is it?

Disaster recovery (DR) involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

It is a sub-function of “business continuity” which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.

What is the primary purpose?

- Reduce the risk your business faces because it is connected to the internet.
- To have a plan that minimizes business downtime in the event of a failure.
- So, people know what to do.

How does it work?

- Plan out the actions the business will take in the event of a disaster.
- From an IT perspective, identify how the business will continue to operate when each system component fails and when the business will cease to operate and how it will handle that event.
- With each system evaluate and decide how to recover from a failure. Evaluate the options, cost, and downtime.
- Implement whatever additional systems that are needed.
- Test the disaster recovery plan.

http://searchsecurity.techtarget.com/definition/antivirus-software

Disaster Recovery

Top backup assumptions that put your business at risk

- I have a backup. I am covered.
- My IT guy has me covered.
- **I will be “back up and running” in a couple hours.**

What do I do?

- Understand what the backup software provides your business.
- Understand what other options you have for disaster recovery to minimize downtime of the business.
- Implement your disaster recovery plan based upon a cost benefit analysis and manage your risk.
- Understand you will have data that needs to be re-entered.
- Understand you will have images that are lost.
- Get objective evidence DR system is monitored (Activity Report).
- Get objective evidence DR system problems are resolved.
- Review the report with your IT service provider until you know how to read it and ask questions.
- Test your DR system on a periodic basis.
- See if you have missed something, update the plan and the system as needed. Be prepared.

Why?

- Because when you are in the middle of a disaster it is too late to start figuring out what to do.
- Minimize downtime and data loss risk to you, your business and your clients.

http://searchsecurity.techtarget.com/definition/antivirus-software

Intrusion Detection Prevention System

What is it?

An **intrusion detection prevention system** (**IDPS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. They will attempt to block suspicious activity then report it.

What is the primary purpose?

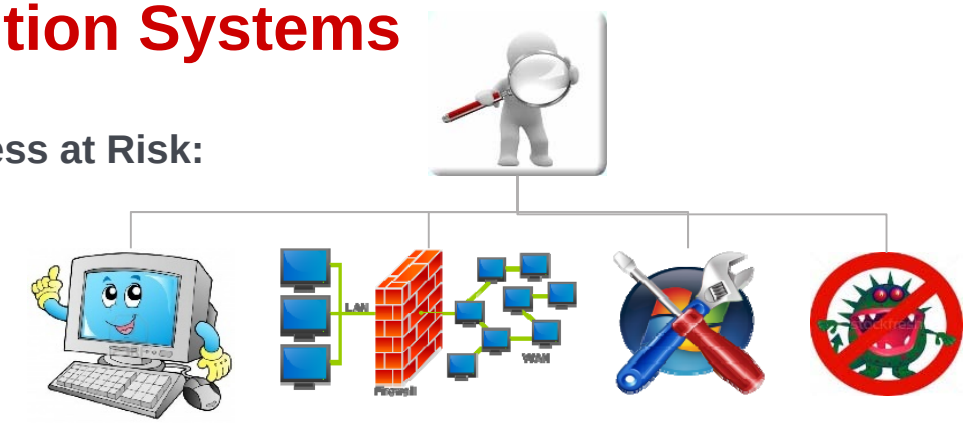
- Reduce the risk your business faces because it is connected to the internet.

How do they work?

- An intrusion detection system monitors a network for threats from the outside.
- An intrusion detection system monitors a network for internal threats and unexpected events.
- Intrusion detection systems are like fire alarms, 2D X-Ray, 3D X-Ray, drawing blood or taking a biopsy.
- It looks at the attack and breach vectors to see if an intrusion event is in progress.

https://en.wikipedia.org/wiki/Network_monitoring

Intrusion Detection Prevention Systems



Top IDPS Assumptions that put your business at Risk:

- I am too small.
- It is too expensive.
- My IT guy has me covered.

What do I do?

- Understand what the IDPS provides your business.
- Understand if your IT company provides a solution, and utilizes a remote management and monitoring agent on your computers.
- Implement an IDPS based upon cost benefit analyses and manage your risk.
- Your objective evidence is contained in the previous sections (Activity Report).
- Review the report with your IT service provider so you know how to read it and ask questions.
- Are they reporting hardware failures before they happen?

Why?

- Minimize risk to you, your business and your clients.

https://en.wikipedia.org/wiki/Network_monitoring

Virtual Private Network

What is it?

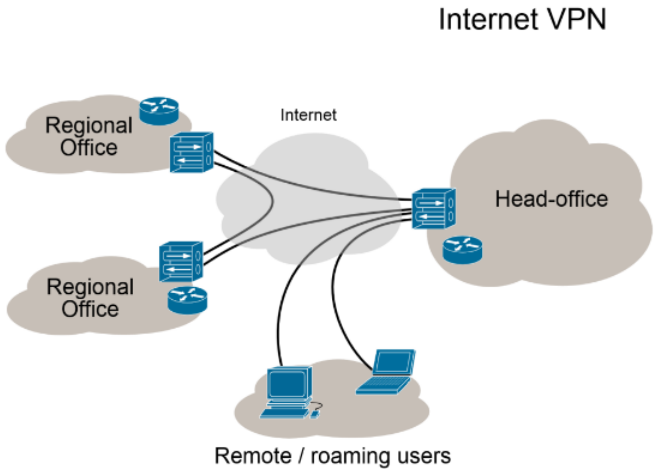
A virtual private network (VPN) is technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources.

What is the primary purpose?

- Reduce the risk your business faces because it is connected to the internet.
- Provide remote users secure access to your system.

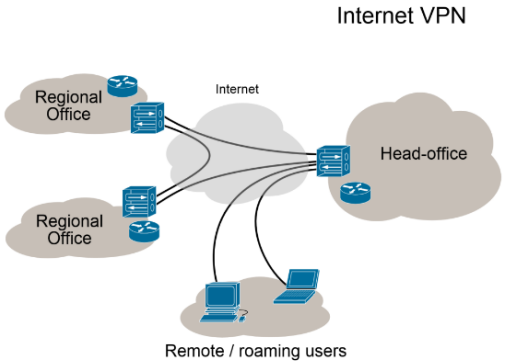
How to they work?

- They encrypt data in transit between the remote location and the office.
- A VPN connects users remotely to the office using encryption technology.
- Applications run across the VPN like you are in the office.
- Either remote client (Software) or point to point tunnel (Hardware)



https://en.wikipedia.org/wiki/Virtual_private_network
https://hacked.com/virtual-private-network-vpn-everything-you-need-to-know/

Virtual Private Network



Top VPN assumptions

- All VPNs are the same.
- All VPNs have the same level of security.
- Using my home computer is safe to connect to the office because it uses a VPN.
- I don't need to maintain my home computer. I have a VPN to the office.
- My IT guys have me covered.
- I have a VPN connection from home. I'm safe.
  - Oops: VPN's connect the computer to the office like it was on the network. If that computer becomes infected it can infect the office computers or provide the attacker with remote control and access to your medical records remotely.

What do I need to do/consider?

- Is remote access needed?
- What other options are available?
- What countermeasures can be put in place to protect against attack and breach within the VPN and remote system?

Why?

- Minimize Risk to you, your business, and your Clients. *(Hum…?)*

https://en.wikipedia.org/wiki/Virtual_private_network
https://hacked.com/virtual-private-network-vpn-everything-you-need-to-know/

Vulnerability Scanning

What is it?

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes.

What is the purpose?

- Reduce the risk your business faces because it is connected to the internet.
- A vulnerability scan detects and classifies system weaknesses in computers, networks, and communications equipment and predicts the effectiveness of countermeasures.

How does it work?

- It looks for security holes within your network systems that can be exploited.
- It is performed by the good guys and the bad guys.
- A script is run across a group of addresses. (This is the drive-by.)
- The responses to the requests are recorded. (This is the drive-by.)
- The responses indicate the attacks that can be performed. (This is the drive-by.)
- The attacker now pulls the appropriate code to attack your system.
- They go after the easy ones first.

http://searchsecurity.techtarget.com/definition/vulnerability-scanning

Vulnerability Scanning

Top vulnerability scanning assumptions that put your business at risk

- Hackers will not find me. I'm too small.
  - Oops: Hackers will just run a script, log the results and attack.

What can I do?

- Have a firewall that is appropriate to network defense needs and is properly configured.
- Do not expose ports for internet based connections to internal systems without protection.
- Build a system of detection, protection, and prevention.

Why?

- Minimize risk to you, your business and your clients.

http://searchsecurity.techtarget.com/definition/vulnerability-scanning

Encryption

Top encryption assumptions that put your business at risk:

- Encryption completely protects me from/during a breach event.
- I encrypt, I don't need to take any other security actions.
- Encryption works on all operating systems.
- Just because you are encrypted doesn't mean they will not try to get in.
- When the system is operational the data is NOT encrypted.
- Don't forget the government has asked to have access to everything overtly.

What can I do?

- Understand the technology and how it manages risk for the business.
- Decide if it is something you want to pursue. (Drive and/or email encryption)
- Utilize encryption when communicating with your businesses to keep communications private.

Why?

- Minimize risk to you and your business.
  - When a drive is lost or stolen.
  - When a computer is lost or stolen.
  - When you want to discard a drive.
  - When you want to communicate something with another business securely.

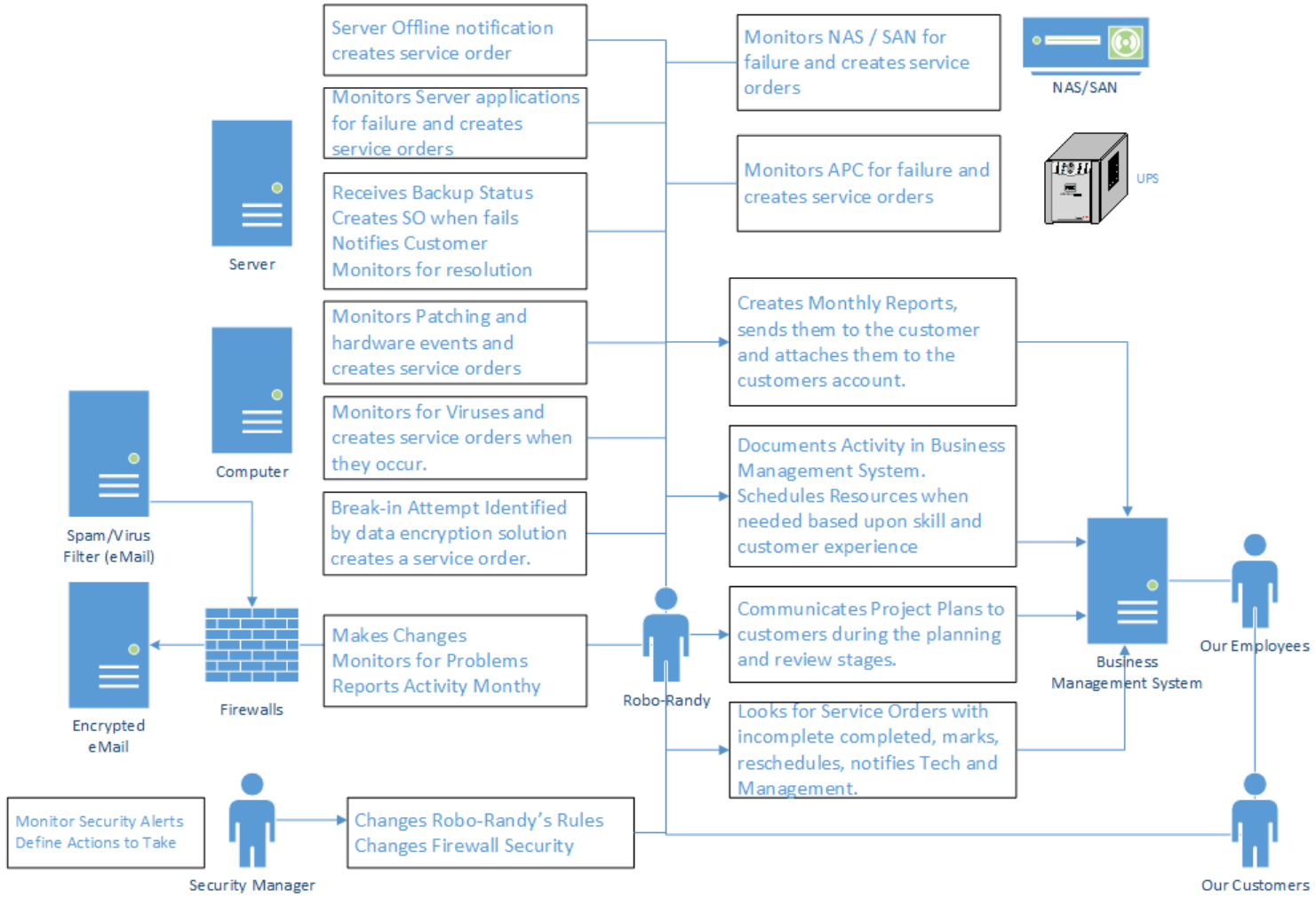
http://searchsecurity.techtarget.com/definition/encryption

Our MSSP System

Our MSSP System…..

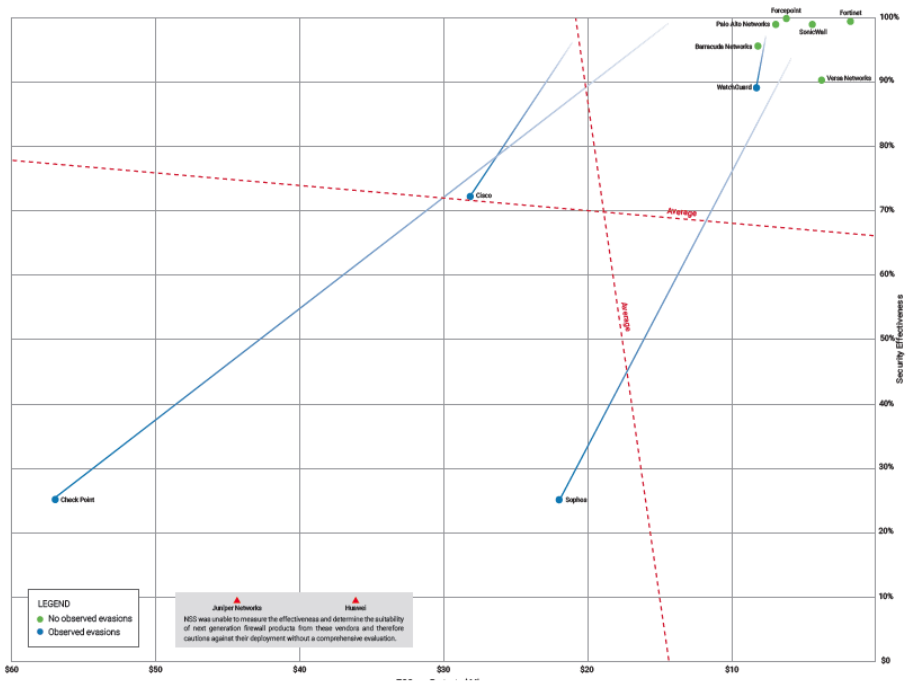
- ✓ Monitors your system for hardware, software and security problems
- ✓ Automatically create service orders
- ✓ Automatically alert and schedule resources to address problems
- ✓ Monitor service orders for closure and escalate when unresolved
- ✓ Report activities monthly to clients to meet regulatory requirements
- ✓ Automatically deploys firewall changes and documents these changes within each customer's account.
- ✓ Why do we partner with Sonicwall, Continuum, Intronis, Appriver, Beachhead, Webroot, ESET etc? Because they allow us to interface our system with their system to create an integrated system that can respond to the ever changing threat landscape we are all faced with.

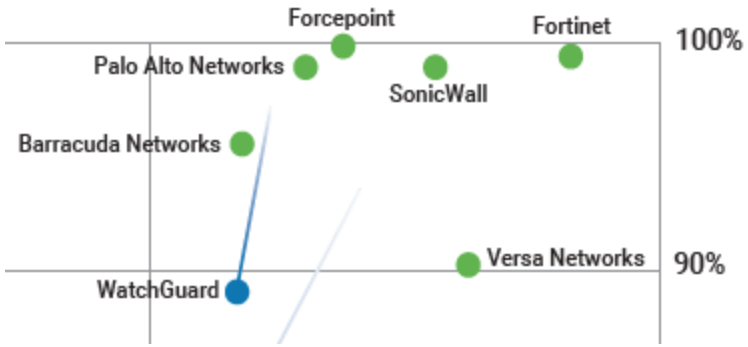
Our MSSP System…..



Our MSSP System…..Why Sonicwall?

Next Generation Firewall (NGFW)





PRODUCTS TESTED

- Barracuda Networks CloudGen Firewall F800.CCE v7.2.0
- Check Point 15600 Next Generation Threat Prevention (NGTP) Appliance vR80.20
- Cisco Firepower 4120 Security Appliance v6.2.2
- Forcepoint NGFW 2105 Appliance v6.3.3 build 19153 (Update Package: 1056)
- Fortinet FortiGate 500E V5.6.3GA build 7858
- Palo Alto Networks PA-5220 PAN-OS 8.1.1
- SonicWall NSa 2650 SonicOS Enhanced 6.5.0.10-73n
- Sophos XG Firewall 750 SFO v17 MR7
- Versa Networks FlexVNF 16.1R1-S6
- WatchGuard M670 v12.0.1.B562953

Q&A

THANK YOU!

Today's Speaker

Randy Mayall
CEO/Security Officer
CCPlus

585-697-0649
rmayall@ccplus-usa.com