



clarity
GAINED

The 10 Critical Emerging IT Security Risks





INTRODUCTION

EVERYTHING IS CONNECTED

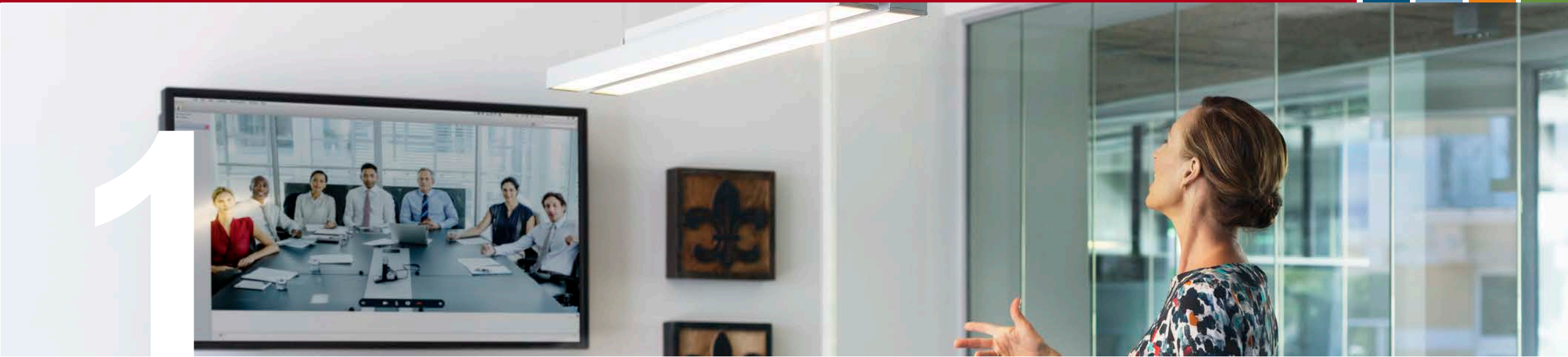
All of our Top 10 risks impact both consumers and professionals

The risks:

- Created from input from all areas of our Firm
- Based on what we see every day
- A blend of healthcare, private sector, governmental, and higher education industries
- Changing regulations

What we'll learn today....

- Overview of the risks
- Potential impact to you and your organization
- Suggestions for mitigating risks



THE INTERNET OF THINGS (IoT)

- The IoT refers to any device that connects directly or indirectly through a Bluetooth connection, to a mothership device, and to the internet
- On a consumer level – Amazon Echo, Google Home, Home security systems, your iWatch and fitness trackers
- In business – conference room systems, healthcare monitoring tools, printing presses, and surveillance systems
- Life is easier, but there is risk....

INTERNET OF THINGS

WHAT'S THE RISK?

Forbes estimates that in 2018, nearly 11 billion IoT devices around the world will be connected to the internet.

- Devices come shipped ready for “plug and play”
- Default Settings – sure it works, but it does for everyone else too
- Connected to your network and the Internet

Hackers can easily “hijack the device” if default settings are not changed. Think of the impact....

INTERNET OF THINGS

IT'S ALREADY IN THE NEWS

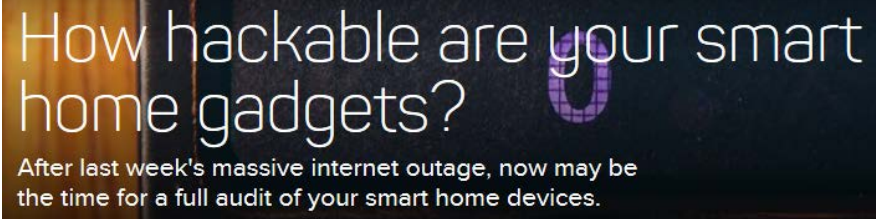
Virtual assistants hear everything, so watch what you say. I'm not kidding

Virtual assistants such as Google Home and Amazon Echo lack security guards, raising questions about safety and privacy



(CNN) — Dallas residents were jolted out of bed late Friday evening after a hacker triggered all the city's emergency sirens, setting off a wave of panic and confusion.

Earlier this month, Johnson & Johnson notified 114,000 diabetic patients that a hacker could exploit one of its insulin pumps. The J&J Animas OneTouch Ping could be attacked, disabling the device or altering the dosage.



INTERNET OF THINGS

WHAT CAN YOU DO?

- Change your password and other settings where possible
- Turn it off when not in use
- Update and re-boot at least weekly

Organizations where devices are used should consider separate and secure wireless networks for devices

Monitor your network for suspicious activity



NETWORK SECURED ONLY AT PERIMETER

IT USED TO BE JUST ABOUT THE FRONT DOOR

- Firewalls at the edge of your network and the Internet were sufficient protection
- Multiple access points now should adjust that thinking
- Threats from the inside
- Your data is not just on your network now

NETWORK SECURED ONLY AT PERIMETER

- Multiple firewalls should be in place throughout the network
- Segmentation – break servers apart by function with strong access rules
- Monitor network traffic throughout systems
- Segregation of duties – much like accounting roles
- Log review and alerting

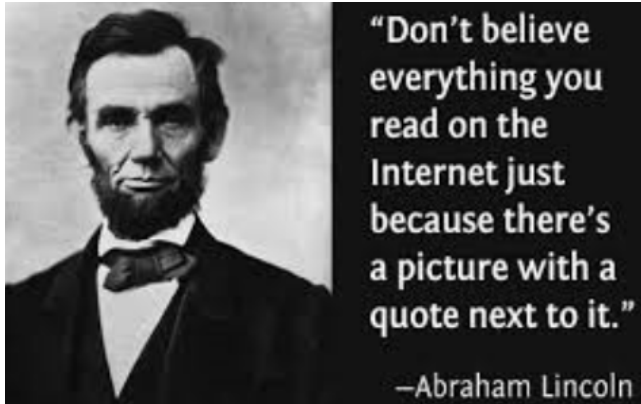
3

THE WORLD OF FAKES

NOT ENTIRELY WHAT YOU'RE THINKING....

- Fake information that gets you to act or click
- Fake ransomware/virus notifications
- Fake helpdesk tickets or calls
- Fake news
- “Deep fakes”
- Social Media accounts

THE WORLD OF FAKES



A 2017 Pew Research study found that 69% of adults in the United States regularly used social media sources to get news

Owner of firm behind fake Tripadvisor reviews jailed in Italy

Landmark ruling by Lecce court over posting of fake reviews results in prison sentence for owner of PromoSalento

Ransomware campaign targets businesses with fake invoice message

Locky ransomware was once of the most prolific forms of ransomware - a new 'PyLocky' ransomware campaign by attempting to piggyback on its past success.

In 2013, \$130 billion in stock value was wiped out in a matter of minutes following an AP tweet about an "explosion" that injured Barack Obama. AP said its Twitter account was hacked. Although stock prices recovered shortly thereafter, this instance points to how news on social media can be manipulated to impact high-frequency trading algorithms that rely on text to make investment calls.

THE WORLD OF FAKES

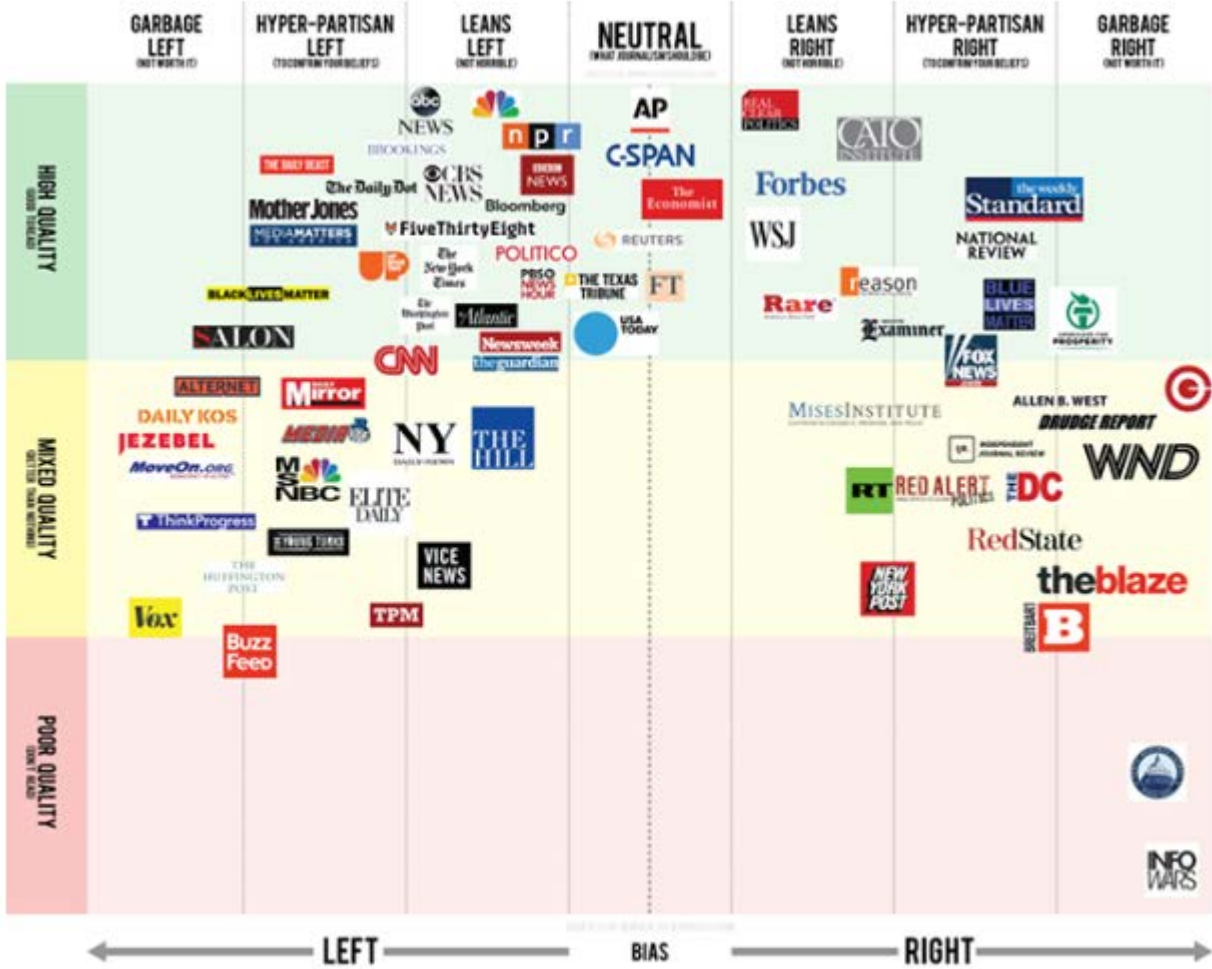
WHAT CAN YOU DO?

Understand the source and think about the context

- Validate through multiple sources
- Run your anti-virus software before you click
- Don't "friend" unknown people
- Set Google alerts for your Organization
- Have a PR plan ready
- There is bias in the media....

THE WORLD OF FAKES

NOT EVERY SOURCE IS EQUAL...



4

SMARTPHONE HACKING

LOST OR STOLEN PHONES

- **95%** of Americans own a smart phone
- 70 million phones are lost or stolen/year – 7% are recovered
- 4.5% of a company's mobile assets are lost or stolen/year

THOSE NUMBERS COMBINED WITH -

- 25% of smart phone owners don't use passcodes
- Continued insistence on merging personal and work use

SMARTPHONE HACKING

A COMBINATION OF RISKS

Other risks and factors -

- Phishing Texts – Text messages seeking to deceit or trick a user
- Scare-ware software – Fake threats that they found illegal material on phone – pay us now to fix it!
- Sniffing software – Software that steals data, such as account information for online banking
- Spam-bots – Software that takes over your social medial accounts and spams contacts –
- Robo-calls. Steal your number!





SMARTPHONE HACKING

WHAT CAN YOU DO?

- Use a passcode!
- Avoid clicking on short links (used on social media most often)
- Only purchase/download applications from trusted sources
- Train employees – banks will never text you for account information
- Use a container application for work email and data
- Maintain ability to wipe employee's phone's that are lost or stolen

5

MERGERS AND ACQUISITIONS

BIGGER IS NOT ALWAYS BETTER

- Big issue in healthcare – merging systems (ERP systems)
- Focus on branding and not on systems (external versus internal)
- Personnel and management changes that cause confusion/conflict
- Lack of testing for integration
- Two sets (or more) of data

MERGERS AND ACQUISITIONS

FAILED SYSTEMS HAVE IMPACTED US ALL

75% of mergers and acquisitions fail due to unsuccessful software system integration.



Catholic Health Initiatives acquired St. Luke's Episcopal Health System in Houston (including flagship St. Luke's Hospital, above) in 2013. The aggressive push into Texas created challenges for the system.

Merger indigestion: Big hospital mergers failing to deliver promised results

By Melanie Evans | April 23, 2016

Hospital operator **mergers** have created big—sometimes behemoth—health systems that will provide the scale necessary to achieve operating efficiencies and compete for more cost-conscious consumers.

Behind each of the four big players in the U.S. airline industry — American, United, Delta and Southwest — there is a tangled computer system pieced together after decades of mergers that married mismatched networks.

MERGERS AND ACQUISITIONS

WHAT CAN YOU DO?

Slow down!

- Understand systems of both organizations – which system will become the “master” or is a new system needed?
- Take inventory of systems, data, and hardware
- Test systems extensively before merging
- Understand roles and personnel

Back it up!

- Run systems in parallel until you are confident the merged system works
- Phase in the merger – department by department approach
- Continuous verification and data integrity checks

6

GOVERNMENT HACKING

THIS IS NOT A NEW CONCEPT...

- Attempts to influence political direction and results of elections
- New kind of a war – crippling infrastructure and supply chains

MORE THAN POLITICS...

- 0-day vulnerabilities known by governments but kept secret
- Those vulnerabilities also impact industry as they are holes in systems and software

GOVERNMENT HACKING

THIS IS IN THE NEWS EVERY DAY

WikiLeaks publishes more secret CIA tools after the US threatens criminal charges



Is the Pentagon Hacking North Korea's Missiles?

Hackers are attacking Word users with new Microsoft Office zero-day vulnerability

The bug affects all supported versions of Microsoft Word, but will be fixed this week.

MOSCOW — The Kremlin on Monday denied accusations that “key elements” of the Russian government had hacked into email accounts at [Denmark’s](#) Defense Ministry over the last two years in a sustained cyberattack.

GOVERNMENT HACKING

WHAT CAN YOU DO?

How do you reduce data leaks and breaches?

- Employee background checks
- Manage access – rule of least privilege
- Know what data you have and where it is
- Monitor internal activity
- Prevent local saving – data grabbing

Patch!

- Don't ignore patches – often these are addressing 0-day vulnerabilities
- Force weekly server re-boots
- Firewalls and Intrusion Detection Systems should be in place



CYBER INSURANCE

- Used in conjunction with risk management – transfer of risk – but there is an over reliance
- Helps with costs of data breach, hacking, reputation loss, and remediation
- Data security is still your responsibility

Understand your policy. What is covered, what are the expectations and responsibilities, and what are the covered events?

CYBER INSURANCE

One survey found the average total organizational cost of a data breach in the US was \$7.01 million dollars. The biggest loss to an organization is the loss of business and customer trust.

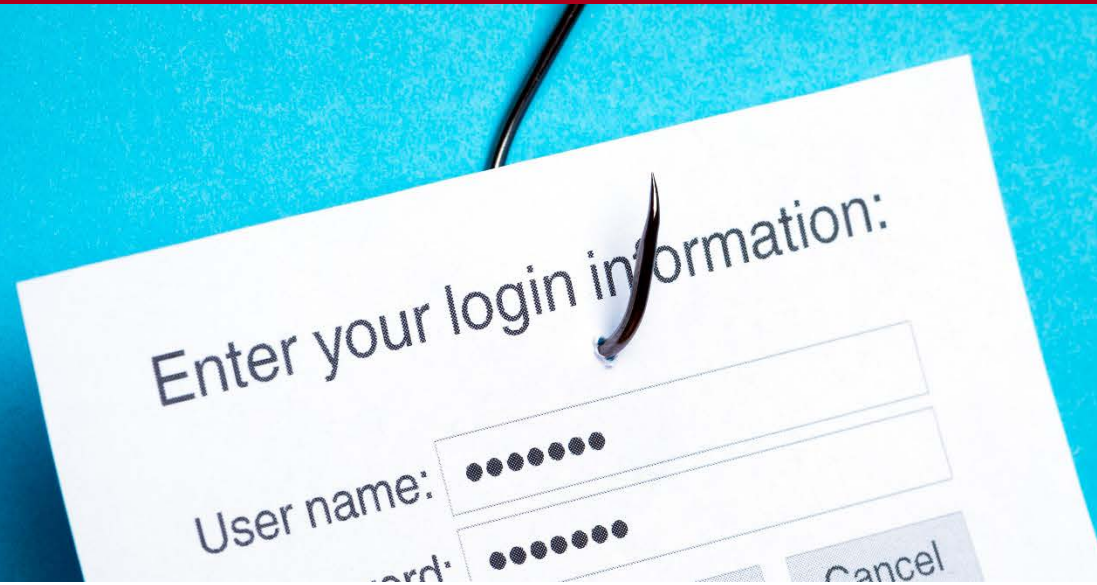
WHAT CAN YOU DO?

- Cyber Insurance is used as a last resource
- Critical to have, but a robust security program should be in place as well
- Backups and business continuity

THINGS TO CONSIDER...

- Does not cover your reputation
- Expensive for good coverage
- Effective if you have the right coverage....Law School Example

8



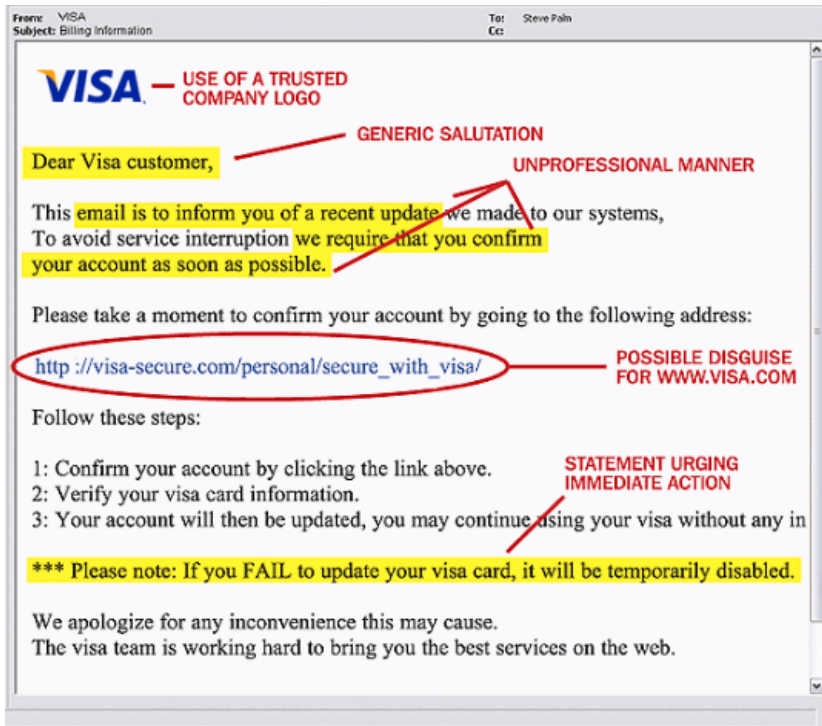
ADVANCED PHISHING SCAMS

THE RISKS ARE ALL RELATED

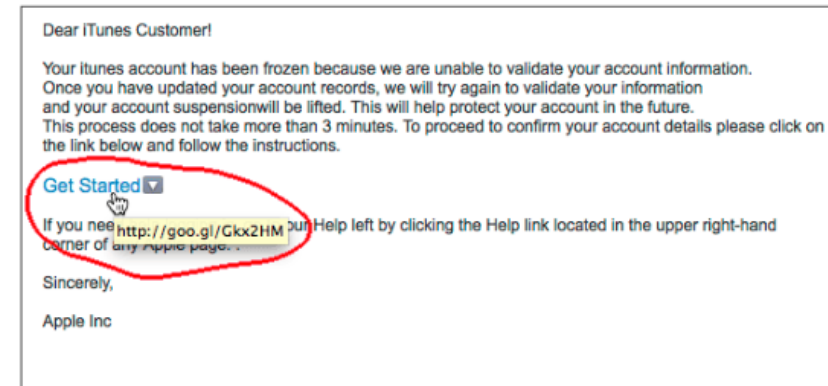
- The world of fakes – deception through realistic appearing texts, emails
- Use of third-parties to “update your claim account information”
- Whaling
- Account information or getting you to download something is the goal
- On the phone now – “I am calling from your help desk”

ADVANCED PHISHING SCAMS

THEY'VE GOTTEN BETTER



From: apple, Inc <Update_account_confirmed@getvistat.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information 1



Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

ADVANCED PHISHING SCAMS

WHAT CAN YOU DO?

TECHNOLOGY

Phishing Is the Internet's Most Successful Con

Tricking people out of sensitive information online is far too easy.

Always be a skeptic.

- If it looks fake, it is fake. Call the company from the number on your card or statement.
- Companies do not email customers over account information
- Hover over the link....
- Security Awareness Training
- Social Engineering Testing
- Email filters, anti-virus, patching

9



LACK OF IT SECURITY RISK ASSESSMENTS

THE FOUNDATION OF EVERYTHING IS RISK

- Risk = Impact x Likelihood to occur
- A risk is the reason you have a control environment – protect assets, reputation, and people
- You cannot secure your systems properly if you do not know where the potential gaps may be
- Regulators require risk assessments



RISK ASSESSMENTS

- HIPAA – OCR Audits
- Financial Controls/ SOC Reports
- Helps with management buy-in for expansion of controls and systems/tools

WHAT CAN YOU DO?

- Risk Management Program
- Pick a framework – CoBit, COSO, NIST, etc.
- Re-visit annually
- This is not an easy nor quick project

10

ADVANCED RANSOMWARE

RANSOMWARE IS IMPACTFUL

- System lockout through encryption
- Entire network encryption and lockout (worm)
- Webpage Denial of Service Attacks

IMPACTS:

- Humiliation of victims – Ashley Madison
- Reputation loss – we locked out Target!
- Loss of business – What if Amazon.com went down for 10 minutes?

ADVANCED RANSOMWARE

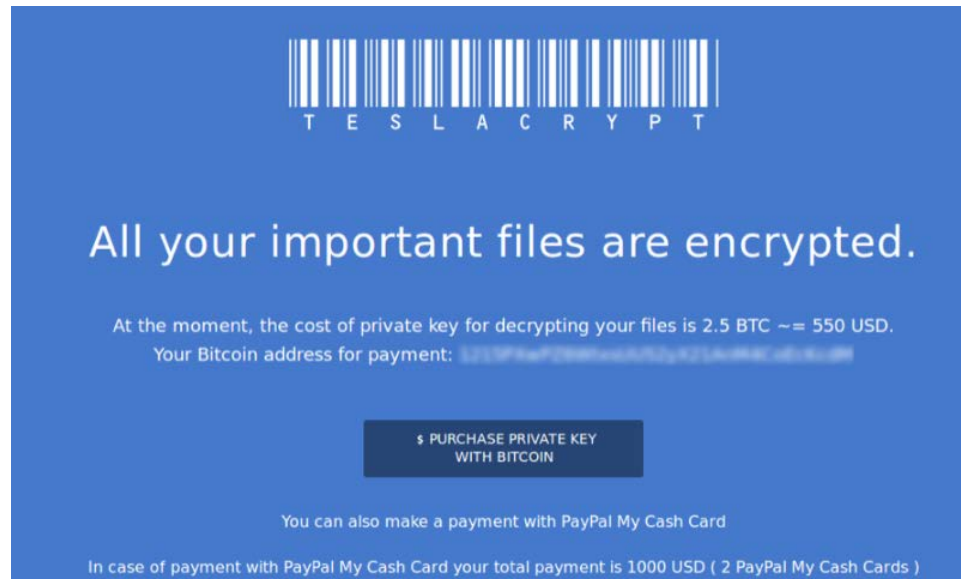
A ransomware attack locked out all the users of the Hollywood Presbyterian Hospital, jeopardizing patient care, until the ransom was paid.

WHAT CAN YOU DO?

- Employee training – STOP CLICKING!
- Take away local administrator use of employee workstations – prevents installation of software
- Backups and patches
- Software whitelisting
- Disable auto-play
- Micro-segmentation
- Email filtering

ADVANCED RANSOMWARE

NOT WHAT YOU WANT TO SEE!



The screenshot shows a blue background with a white barcode at the top. Below the barcode, the word 'TESLA CRYPT' is written in white capital letters. The main text reads: 'All your important files are encrypted.' Below this, it states: 'At the moment, the cost of private key for decrypting your files is 2.5 BTC == 550 USD. Your Bitcoin address for payment: 1234567890123456789012345678901234567890'. There is a dark blue button with white text that says '\$ PURCHASE PRIVATE KEY WITH BITCOIN'. Below the button, it says 'You can also make a payment with PayPal My Cash Card'. At the bottom, it says 'In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards)'.



The screenshot shows a black background with red and white text. At the top, it says 'YOUR COMPUTER HAS BEEN LOCKED!' in red. Below this, it reads: 'This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected: Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer. This computer lock is aimed to stop your illegal activity.' To the right of the text is a circular seal of the 'DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION' with a central shield and stars. Below the seal, there is a white input field and an 'OK' button. The text continues: 'To unlock the computer you are obliged to pay a fine of \$200. You have 72 hours to pay the fine, otherwise you will be arrested. You must pay the fine through [redacted]. To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK!.'



INTERESTED IN MORE?

CONTACT:

Christopher S. Ellingwood

cellingwood@berrydunn.com

207.541.2290