Critical Cyber Threats to your Facility in 2020

Ron Lander, CPP, CMAS, CHEPS, PSM
Capt. Werner Preining, CPP, CMAS
Keith Flannigan, PhD, CMAS, CHEPS, CFE
Welcome to GSX 2020

• Please place your cell phones on vibrate!
• Please complete the evaluation for the session.
• This is Session number 4303
• If you would like to have a copy of the presentation leave your business card.
• If you pass your business card forward, we will be having a drawing for door prizes. If you do not have a card write your email address and name on a piece of paper and send it up.
• Thank you for coming.
What you can expect in the **near** future

- Each year the attacks on our networks and IT Systems increases in both frequency and complexity of attack.
- These criminals are better trained with better equipment and more knowledge.
- The use of A.I. in Cyber Attacks is increasing daily.
- This presentation will be providing you with information on what you can expect to address in the next year.
Protecting your network from Cyber Attacks in 2020

• Projected losses from Cyber Attacks in 2019 will be over 2 Trillion Dollars.
• Increase of over 1 Trillion dollars from 2017 losses.
• Attacks and threats are increasing each month.
• While we are busy working and earning for our families these criminals are staying awake nights drinking Red Bull and Mountain Dew while dreaming up new ways to attack our facility networks to steal our data or money.
IT Directors Loss of Sleep

• Hackers gain access to your system, stealing mission-critical information, locking sensitive files, or leaking proprietary information to the public.

• While you are sleeping there are 1000’s of hackers drinking Red Bull and dreaming up new ways to compromise your system.
30,000 data records Stolen per minute

• In the last month, there have been over 700,000,000 records breached.
• In one case alone 127,000 personal data information records were put up for sale on the Dark Web.
• Hospital medical records being ransomed, bank account information being deleted, medical MRI records being altered to show tumors on x rays or MRI’s, or removing them from the file.
Equifax $4 Billion Dollar Initial Stock Loss

• Equifax data breach quickly moved up the ranks as one of the worst cyber security attacks in history after the personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers’ license numbers) of 143 million consumers was exposed.

• Additional losses come in the form of paying for credit monitoring, postage, advisement mailings, legal fees, settlements and court cost.
Attacks on Police Officers

• Personal Information Of Thousands Of LAPD Officers & Applicants Exposed By a Single Data Breach.
• City officials say they are investigating a data breach of the personal information of thousands of Los Angeles Police Department officers.
• DOB, Passwords and Email Addresses
• Recent Texas Ransomware Attacks
Phishing attacks are up over 60% in 2019 over 2018

- Each year the various types of attacks have increased.
- This year, Phishing attacks are up over 60% from 2018.
- You can expect them to continue to increase exponentially.
- Employees need to be briefed and trained on this very dangerous topic.
Average Data Breach Cost $1.3 Million Dollars

- Even if you do not have a huge company you will still suffer damages from:
  - Reputation Damage,
  - Federal Fines or Sanctions,
  - Loss of Data,
  - Loss of Credibility,
  - Loss of Income,
  - Loss of Productivity
  - Second Order Effect!
Various Types of Cyber Attacks

The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*

Your computer → On the way to a website

DNS Domain Name System

Malware
"Malicious software" such as ransomware, designed to damage or control a computer system

Phishing
Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Source: Techterms.com, Lloyds of London, Forbes*

Man-in-the-Middle Attacks
Hackers insert themselves between your computer and the web server

Cross-Site Scripting
Injects malicious code into a website which targets the visitor’s browser

DDoS
Distributed Denial of Service: a network of computers overload a server with data, shutting it down

SQL Injection Attack
Corrupts data to make a server divulge data, such as credit cards numbers, usernames

© AFP

GSX.org | #GSX19

SOLUTIONS MULTIPLIED.
Ransomware

• Ransomware is the High Jacking or Kidnapping of your data.
• The hackers will use some form of phishing, in which a user in your system receives an email with a malicious file attached.
• It looks completely legitimate, like something they receive every day.
Opening the File Deploys the Ransomware

- Opening of the file results in the encrypting and locking specific, highly sensitive files on the user’s computer or your servers.
The Dreaded Message

- When the user attempts to open the files, they are confronted with a message stating that their files have been locked, and that they will only receive the encryption key if they pay a specified amount to the hacker, usually through an untraceable Bitcoin payment.
Attacks Increased over 2,500 % this year!

• This type of attack is massively on the rise, with ransomware attacks increasing over 2,500 % last year.
• In the first 6 months of 2019 there have been over 200,000 ransomware attacks.
Who is Being Attacked by Ransomware?

- Anyone Could be Attacked but those that require quick access to their data files are most at risk.
- Banks
- Medical Facilities
- Government Agencies
- City and State Government
- Law Enforcement
- Military
22 Gov Agencies have Been Attacked in 2019

- Here’s a sampling of ransomware attacks that have hit specific cities, towns and government organizations. Keep checking the list for ongoing updates:
  - June 26, 2019: Lake City, Florida agrees to pay ransomware.
  - June 20, 2019: Riviera Beach, Florida, discloses ransomware attack and payment.
  - May 7, 2019: City of Baltimore hit with ransomware attack.
  - April 2019: Cleveland Hopkins International Airport suffered a ransomware attack.
  - April 2019: Augusta, Maine, suffered a highly targeted malware attack that froze the city’s entire network and forced the city center to close.
  - April 2019: Hackers stole roughly $498,000 from the City of Tallahassee.
  - March 2019: Jackson County, Georgia officials paid cybercriminals $400,000 after a cyberattack shut down the county’s computer systems.
The Ultimate Hacking Ransom, Your Pacemaker

• With the new 5G systems it will allow people to monitor you everywhere that you go.
• Any electronic medical device that you may have inside or attached to your body can be hacked and changed or stopped.
• Pacemakers, insulin, pain meds all could be subject to hacking.
• There has been one known murder of a man having his morphine drip increased and causing him to OD.
5G Access to Your Vehicle

- With the 5G system providing total coverage it allows hackers to find new targets.
- They could hack your vehicle and shut it off causing you to have to pay to be able to regain access to driving your car.
- System could also be used to disable various functions of the vehicle such as the brakes, air, GPS or windows.
- They could also take over driverless cars and use them as vehicle weapons.
To Pay or Not To Pay

• If you PAY:
  • Bad Publicity
  • Open to New Attacks
  • Risk of the Files Not Being Unlocked.
  • Risk of Files Being Corrupted

• If you DO NOT PAY:
  • Loss of Critical File
  • Loss of Funds
  • Publishing of Proprietary Information
  • Releasing of Customer Information
Internet of Things

The Internet of Things is made up of all the digitally connected items that, in the past, have never been able to connect to the internet.

- Appliances
- Security Cameras and Systems
- Lights, Door Locks
- Thermostats
- Garage Door Openers
- Speakers,
- Coffee Pots, Slow Cookers
IoT has Many Security Flaws

• Being new the IoT still has many areas of vulnerability that are being exploited by hackers.
• As millions of more people begin to utilize the 1000’s of available IoT items such as Alexa or Siri the risk of attack increases.
• A mass attack coordinated against hundreds of IoT devices could be catastrophic.
• In 2016 a Mass IoT attack shut down HBO, Fox, PayPal and many more.
Over 25,000 IoT Items in the Workplace

- The IoT is now over 25,000 items and many being utilized in the workplace.
- The majority of these items are not secured, and many people and businesses utilize these items leaving their offices and homes vulnerable to attack or denial of service.
3/4th of Companies do not address IoT Security

- A recent survey states that over 60% of companies fear an IoT ecosystem ransomware attack.
- Only 28 percent say they currently include IoT-related risk as part of the third-party due diligence.
- Expect this to be one of the prime areas targeted by hackers in the next few years.
DSLR Cameras Vulnerable through WiFi Connection

- Security researchers were able to remotely install malware on a digital DSLR camera.
- It was found that a hacker can easily plant malware on a digital camera.
- Infected Wi-Fi access point could deploy it at a tourist destination to pull off an attack or infect a user’s PC.
- The same attack software can be used against your security cameras.
Embarrassing Photos or Information

• Cameras could be a particularly vulnerable target for hackers: they’re full of personal images that most people likely won’t want to walk away from.

• There could be either irreplaceable photos or embarrassing photos that you would be willing to pay to keep private.

• Camera is linked to your computer or phone compromising your network.
Social Engineering and Phishing

- Social Engineering has been around since the beginning of time...because it works.
- Social Engineering works because most people are gullible and easy to trick.
- Like J.P. Barnum stated “There is a sucker born every minute.
- Hackers trick people into thinking they are giving information to a legitimate person or institution.
One Example of Social Engineering

• I had a case that a person sent magnets and mouse pads with an 800 number to businesses. The accompanying letter stated that they were the new Tech Support Company for their computers.
• They then waited for someone to have an IT problem and let them call the 800 number.
• The caller thought that they were talking to a legitimate Tech Support and provided them with their login and password.
• The hacker then told them that their computer was not repairable and would send them a new computer and wait for the next sucker to call.
Another Example by Requesting a Password Reset

• A hacker may email employees at your company, posing as a system administrator, asking them to reset their password.

• A link is included in the email that directs the employees to a page that *looks like* one of your legitimate password reset pages, including fields for the username and old password.

• When the employee enters their old password, the hacker gets access to what is actually their current password. They can then immediately log into your system without any detection.
Phishing Attacks Following a Data Loss

• Hackers often launch these attacks in the wake of legitimate security breaches.
• People who would normally never fall for such a scam are much more liable because they know there was a security breach and that password resets are standard protocol following a breach such as an email from Bank One after the Bank One Data breach was all over the news.
Phishing Works so it Will Continue

• Phishing attempts are up 65% over the last year
• 76% of businesses reported being the victims of a phishing attack
• Phishing rates are increasing across all industries, meaning no business is immune.
Attacks Will Continue as Long as People do not Pay Attention and Remain Aware

• Employees have been told for 10 years not to open attachments or links without first checking to see who sent it, but 29% of attacks come from opening infected links or attachments.

• There will always be ways to deceive people, but you must brief your staff and employees on these common tactics.
Drive-by Download of Malicious Code

• In the past, a simple way to ensure that you didn’t contract a computer virus was to not download files from any source you didn’t trust.

• A drive-by download is a form of attack that allows malicious code to be downloaded from an internet site through a browser, app, or integrated operating system without any action on the user’s part.

• These URLs are designed to look and act like real websites, but in fact, they are breeding grounds for several different types of malicious code in hopes that one of them will get through your system’s security.
APT Attacks

- APTs (Advanced Persistent Threats) are a form of cyber attack where an unauthorized attacker code enters an unsuspecting system network and remains there for an extended period undetected.
- APTs will quietly sit, stealing financial information and other critical security information.
- APTs use a variety of techniques to gain initial access, including malware, exploit kits, and other sophisticated means.
- Once login credentials are discovered, APTs can scan and infect deeper parts of the infected system, inevitably compromising all forms of data and easily navigating between connected networks.
Recognizing and Defending Against APTs

• While these forms of attack are difficult to detect, there are some key indicators that system administrators can notice to help identify and counter APTs.
• Look for unusual patterns in network activity or large amounts of data access, outside the normal range for the business.
• IT professionals can improve defense by segmenting the network to isolate critical data.
• Utilize honeypots to trap internal attacks.
• Utilize application-specific white lists to limit data access to only the few applications that should be allowed.
Exploit Kits

- These kits are self-contained and sold on the dark web.
- The attack is planned to work in several stages starting with a scan of the user’s system once they navigate to a landing page.
- If vulnerabilities are discovered, the compromised website will then divert web traffic to an exploit and eventually the malicious payload.
How Exploit Kits work and what they do

• Exploit kits are designed to be discreet, so discovering them as they are executed requires the same techniques used to defend against other sources of worms and viruses.

• Software solutions include antivirus and intrusion prevention systems, and human solutions include anti-phishing training for users.
Monokle infected Android devices, but evidence suggests iOS versions may also exist.

• Monocle uses several novel tools, including the ability to modify the Android trusted-certificate store and a command-and-control network that can communicate over Internet TCP ports, email, text messages, or phone calls.

• The result: Monokle provides a host of surveillance capabilities that work even when an Internet connection is unavailable.
The RAT (Remote Access Trojan) is able to:

- Retrieve calendar information including name of event, when and where it is taking place, and description
- Perform man-in-the-middle attacks against HTTPS traffic and other types of TLS-protected communications
- Collect account information and retrieve messages for WhatsApp, Instagram, VK, Skype, imo
- Receive out-of-band messages via keywords (control phrases) delivered via SMS or from designated control phones
- Send text messages to an attacker-specified number
- Reset a user’s pincode
- Record environmental audio (and specify high, medium, or low quality)
- Make outgoing calls
- Record calls
- Interact with popular office applications to retrieve document text
- Take photos, videos, and screenshots
- Log passwords, including phone unlock PINs and key presses
- Retrieve cryptographic salts to aid in obtaining PINs and passwords stored on the device
More on Monokle

- Accept commands from a set of specified phone numbers
- Retrieve contacts, emails, call histories, browsing histories, accounts and corresponding passwords
- Get device information including make, model, power levels, whether connections are over Wi-Fi or mobile data, and whether screen is on or off
- Execute arbitrary shell commands, as root, if root access is available
- Track device location
- Get nearby cell tower info
- List installed applications
- Get nearby Wi-Fi details
- Delete arbitrary files
- Download attacker-specified files
- Reboot a device
- Uninstall itself and remove all traces from an infected phone
How to Prevent Monokle and others

• Do NOT ROOT your phone
• Check the APP that you are loading
• Check the REVIEWS on the APP before loading
• Do not install THIRD PARTY software
• Be DILIGENT with your phone!!!
• PREVENT PHISHING
  • https://phishingquiz.withgoogle.com/
Cracking is when hackers use high-powered computer programs to systematically enter millions of potential passwords in the hope of “cracking” some of the easier ones.
Utilize Strong Passwords and Don’t put it on a Post it Note on your Monitor!

• And we all know that millions of people still use laughably simple passwords, including the ones they use to log in to your system. We’re talking passwords like:
  • “Password”
  • “Abc123”
  • “111111”
  • Their own name
  • Their birthday
35% of People use “Weak” Passwords (?)

- A recent study showed that a staggering 35% of people have what are considered to be “weak” passwords. These are easily crackable passwords.
- Most of the other 65% use passwords that *can* be cracked, given enough time.
Powerful Cracking Programs Available

- As computers grow increasingly powerful, cracking programs can quickly generate billions of potential passwords to try.
- If passwords aren’t sophisticated enough (i.e. they don’t contain enough random characters), they can still be somewhat easily cracked.
Strong Passwords are a Necessity

• While there will always be someone trying to attack your system it is imperative that you require a high level of security with your passwords.
• A weak password is an absolute way to let attackers into your website through the front door.
As an Example of Cracking Facebook

• In fact, you don’t even have to be a professional hacker to get into someone’s Facebook account.

• It can be as easy as running Firesheep on your computer for a few minutes.

• In fact, Facebook actually allows people to get into someone else’s Facebook account without knowing their password.

• All you have to do is choose three friends to send a code to. You type in the three codes, and voilà — you’re into the account. It’s as easy as that.
Man in the Middle Attacks

• We have all heard the old saying that “Nothing in Life is Free” or that there are “No Free Lunches” this is particularly true in the Cyber world.

• Studies found that all 10 of the top 10 “Free” flashlight apps for phones had malware.

• It cost money to develop software. If someone is giving it away for free it is a good bet that you will pay in some way later.

• As we have seen with Facebook and other social media sights that are free they make their money selling your data.
Putting themselves in the Middle

- A man in the middle attack occurs when the attacker finds a way to position themselves between two connecting or communicating devices.
- The attacker “Spoofs” the opposite party so that all parties believe that they are actually talking to the expected other legitimate parties.
“Free” WiFi is a Common Method of Access

- There are dozens of ways that Fake WiFi hotspots can be set up.
- Hackers will use these methods to gain access to your system.
- There is a software tool that request access to your cookies and it utilizes your cookies from other sites to determine your password.
Setting up a Fake WiFi in a Public Location ie; Public Access Atl Airport Wifi, Of Starbucks WiFi

• If you can get close to your target, you can trick them into connecting to a fake Wi-Fi network to steal credentials via a Man In The Middle (MITM) attack.

• Tools like the Wi-Fi Pumpkin make creating a fake Wi-Fi network is as easy as sticking a $16 Wireless Network Adapter on the $35 Raspberry Pi and getting close to your target.

• Once the victim connects to your fake network, you can inspect the traffic or route them to fake login pages.

• You can even set it to only replace certain pages and leave other pages alone.
How to Protect Yourself

• Don’t connect to any open (unencrypted) Wi-Fi Networks.

• Especially don’t connect to any Wi-Fi networks that are out of place.

• Why might you see a “Google Starbucks” when there’s no Starbucks for miles?

• Hackers know your phone or computer will automatically connect to it if you have used a network with the same name before.
Do Not Sign In for Firmware Updates from Free Wifi

• If your router asks you to enter the password for a firmware update to enable the internet or shows you a page with major spelling or grammar errors, it is likely you’re connected to a fake hotspot and someone nearby is trying to steal your credentials.
Corporate Network Vulnerable by Mobile Device

• While there are certainly precautions that can be taken against this, such as installing VPN software on employee computers, there’s still the risk of information being captured from personal devices, such as tablets and mobile phones.

• Be sure to secure personal mobile devices.
Crypto Currency Hacks

• Throughout the past six months, seven crypto exchanges have reportedly seen large-scale hacking attacks to the tune of tens of millions of dollars, with the most recent platform to suffer a security breach being GateHub.

• As the global crypto exchange market continues to see an increasing number of security breaches leading to the loss of user funds, investors may become reluctant to rely on centralized exchanges to store funds.
Slack Bots

• There are many slack bots which are being used by hackers. Since mid-2017, there have been many cases of stolen cryptocurrency through this technique.

• The bot sends a notification to the user’s device about issues with their wallet. The ultimate goal is to force the user to click the notification and type private key.

@slackbot 7:00 PM, July 5th
@imstatusbot asked me to remind you “ALERT: We have been informed by Myetherwallet that there is an error with the Status tokens database. Please visit Myetherwallet.com/?wallet-info?status=token to check your tokens balance and update your contract. Failure to do so may result in loss of Status tokens. Thank you for your cooperation and understanding.”.
As with all types of Cyber Crime: Phishing and Social Engineering are always a Threat

- Cybercriminals also ramp up their focus on social engineering to steal cryptocurrency from newbie users. Fraudulent websites and paid ads are still on the rise even after the ban.
- Hackers mimic the authorization pages of exchanges and dupe users to enter the private key. To avoid it:
  - Enter the exchange address directly to the URL bar
  - Never trust ads offering free cryptocurrencies
CRYPTOCURRENCY MINING BOTNETS

• ‘Botnets’ are networks malware-infected systems which can be controlled remotely. Generally, botnets are used to distribute malware or to perform DDoS attacks.

• There have been many situations where Crypto-criminals are using it to mine cryptocurrency.
SMS AUTHENTICATION

• Most of the users have mobile authentication as it is easy to use and they always have the smartphone.
• But using the SS7 protocol hackers can intercept an SMS with a password confirmation.
• Here’s the vulnerability is in the cellular network. To avoid it:
  • Stop using SMS verification
  • Use software base 2FA
1000’s of Dark Web offers to sell Crypto Hack Tools

- The bad news is there is no decrease in the activity of crypto hacking.
- As per JAN 2019, there are more than 11000 dark web platforms selling more than 34000 offers.
- Here anyone can get malicious software for an average price of $240.
Hacking Tools Available on the Dark Web

MALWARE OFFERINGS

AVAILABLE LISTINGS

0 10000 20000

0 4 8 12 16 20

Stealer Malware  Covert Mining Malware  Mining Botnet  Bitcoin Dealers  Mobile Phone Malware  Miscellaneous Offerings
Crypto Currency Scams

• There is 9 Million dollars a day lost to crypto currency scams and climbing.
• There are many of the same type of scams that impact hard currency thefts.
Crypto Ponzi Schemes

• Last year there were 174 crypto currencies closed down and their originators arrested.

• There are many crypto currency owners that withdraw the hard money from the accounts immediately upon its deposit.

• Once the hard currency is deposited into the crypto account it is impossible to cash out as hard currency.

• Many of these fraudulent cryptos are hosted in African Countries with not way to prosecute the owners.
Pump and Dump Crypto Style

- With the Crypto currencies it has been found that the originators open the currency but also open 2 or 3 websites to allegedly exchange the Cryptos for hard currency.
- The exchange websites show the cryptos being traded and cashed out at a high rate of exchange.
- This is what the sellers of the Crypto's use to legitimize their cryptos and give them value to the purchaser.
Crypto Exchange Theft

- Crypto Currency exchange Mt. Gox.
- This was an early cryptocurrency exchange that at one point accounted for over 70% of all bitcoin transactions worldwide. In February 2014, Mt. Gox suspended trading.
- It later emerged that 850,000 bitcoins had been stolen (valued at $450 million at the time)
- Do not keep your cryptocurrency stored on an exchange. Transfer coins to an offline wallet at the end of the day.
- If you intend to become an active trader, consider upgrading to a cryptocurrency hardware wallet.
Crypto Exchange Fee Money Laundering

- Extreme fees such as recent fees charged by Ethereum
- Insanity: Ethereum Wallet Pays Nearly $575,000 in Fees to Transfer $25 in ETH
- It is suspected that the huge fees are related to a method of Money Laundering
- The minimal transfer is designed not to trigger any reporting of the transaction and then the real transaction is the money sent in fees
ICO’s

• Initial Coin Offerings (ICOs) are the IPOs of the cryptocurrency world.
• Cryptocurrency startups create initial coin offerings to raise substantial amounts of money.
• Many of them vastly overestimate the value of their start-up.
• Others are simply elaborate pump and dump schemes.
• As with any initial offering, investing is a risk, so due diligence should always be applied.
ICO Red Flags

• Red flag indicators might be;
• There is a lack of accurate or current information about a company.
• Questions arise concerning the accuracy of publicly available information, including press releases and media coverage.
• There are questionable trading practices, such as insider trading or market manipulation.
Sale of Coins

- There have been many cases of individuals selling face “Coins” to unknowing buyers.
- They go online and show the price per coin and then tell a story about a sick child or other crisis which is causing them to sell the coins at a greatly discounted rate.
- They are depending on the ignorance of the coins and the greed of the person buying the coins.
- This has happened in the UK and US.
Crypto Currency Being Declared National Security Issue

- U.S. president Donald Trump sent shockwaves through the bitcoin and cryptocurrency community last week when he branded bitcoin "based on thin air,"
- "This is indeed a national security issue," Mnuchin told reporters at a press conference yesterday. “Cryptocurrencies such as bitcoin have been exploited to support billions of dollars of illicit activity like cyber crime, tax evasion, extortion, ransomware, illicit drugs, and human trafficking," adding that Facebook's Libra "could be misused by money launderers and terrorist financiers."
- Echoing Fed chair Jerome Powell, Mnuchin said he is "not comfortable" with Facebook's plans for its private cryptocurrency, Libra.
Beware of Regulations on Crypto Currency

- When the U.S. President, the Secretary of the Treasury and the head of the Federal Reserve all make statements that Crypto Currency is a National Security Issue and Money Laundering it will only be a matter of time before there is legal action taken against those holding Crypto Currency.
- There have been hundreds of Crypto Currency owners arrested around the world.
- One recent report from the IRS stated that anyone who has a numbered financial account that does not have their name connected to the account is attempting to evade taxes.
- There are also reports of banks working with the authorities to provide information when the crypto currency owner brings it to the bank to cash out.
As ML and AI become more readily available to the masses, hackers are using them to enhance the sophistication of their attacks.

With these tools, attacks can be multiplied, and cybercrime can reach all-new heights.

We’re already seeing the evidence! Many of the recent widespread ransomware attacks are ML- and AI-driven.
WordPress Specific Attacks

• WordPress powers approximately 30% of the internet.
• One area of particular vulnerability is third-party plugins. If these aren’t updated on a regular basis, they can introduce risks to your system. A recent study by Securi noted that 25% of hacked WordPress sites were exploited because of out-of-date plugins.
Being Largest Website Software they will be targeted more as the software is better known.

- WordPress sites that don’t use SSL certificates are vulnerable when being accessed through unsecured networks.
- Hackers on the networks can use Man In The Middle attacks to sniff out login details, then login into the site and deface it.
- Disable pingbacks so your site can’t be victim of a DDoS botnet.
What you should do to Protect your Site

- There are number of basic precautions that can and should be taken regarding security, such as regularly training employees on the basics of security, forcing employees to use VPNs on all work-related devices, implementing the latest security software, etc.

- Utilize such techniques as a dynamic web application firewall, chroot user separation, real-time malware scanning, and full restoration processes in the event of a breach.

- Don’t settle for half-measures.

- When they fail, the costs are enormous, and you’re left to pick up the pieces.
Thank you for attending

• Be sure to complete your evaluation forms.
• If you would like a copy of this presentation or if you would like a copy of our presentation on Protecting your Network while away from the corporate campus you may email: KeithFlannigan@ATABonline.org, rlander@ultra-safe.com
• or leave your business card.