Digital Due Diligence…Your Role in Modern Cybersecurity

Co-Chair Allan Reiter – Nex-Tech

Committee Member Christian Hansen – Baker Tilly

In cybersecurity, we do not fight a single wave, we face a relentless tide.

Welcome to the WTA CyberTech Committee Presentation

- Recent and relatable cybersecurity events. What did we learn?
- What should you do and are you prepared?
- Do you know your role?
- NIST Cybersecurity Framework
- Supply Chain Security
- AI Security, Usage and Policy
- What should you do when you get home?

The Colonial Pipeline Attack

<u>May 7, 2021</u>

- Darkside from Russia.
- Assumed compromised VPN password.
- Deployed ransomware.
- They paid 75 bitcoins valued at $4.4 million. Worth more than $8 million now.
- They did recover after receiving decryption keys.
- FBI later recovered most of the bitcoins.

What did we learn from this?

- Passwords, and even complex passwords, are not enough.
- We must implement MFA on VPNs or any external access to internal resources.
- You cannot trust hackers, as some of the exfiltrated data was released later.
- There have been other recent VPN vulnerabilities like the SonicWall CVE-2024-470766. Enforcing MFA and using strong passwords were part of their guidance.
- This disrupted the fuel supply chain and caused brief spikes in fuel and some panic buying, with no stated loss outside of ransom, which most of that was recovered.

Kansas Supreme Court Attack

<u>October 12, 2023</u>

- LockBit associated with Russia.
- They have not publicly disclosed how they got in.
- They deployed ransomware and stole approximately 150,000 peoples' personal information.
- They wanted money, but Kansas did not pay.

What did we learn from this?

- Starting to see a trend here with Russian-related attackers.
- They always take valuable data to hold as hostage.
- Encryption of data so you must restore or recreate.
- With Kansas not paying the ransom, they did not get the keys from LockBit, and it took parts of their system offline for weeks and months.
- Estimated at more than $2.6 million in recovery costs.
- Some wonder that as the FBI obtained thousands of LockBit keys, if maybe the Kansas keys were not provided to them as well.
- Not stated how they got in, but humans sometimes are the weak link.

Oldsmar, Florida, Water Treatment Plant

February 5, 2021

- No one claimed responsibility.
- Remote control using TeamViewer.
- No motive was ever publicly released.
- No data exfiltrated.
- Changes were reversed before causing harm.

What did we learn from this?

- There can be a lot of unknows that may never be known.
- It is not a good idea to have controls for your water treatment plants, or maybe some of your network controls, with remote control software.
- The person observed the computer changing the sodium hydroxide levels. The levels were changed back and remote software disabled.
- Since 2021, there have been reports that this might not have even been a cyber incident and might have been due to employee error.
- It is not always as it appears, but you should separate OT from IT.

Change Healthcare Cyberattack

<u>February 21, 2024</u>

- It is believed that ALPHV was responsible.
- Citrix remote access with no MFA is said to be the entry point.
- They stole data and deployed ransomware.
- They paid $22 million in bitcoins.

What did we learn from this?

- More Russians were likely involved.
- More data was stolen.
- Approximately 192 million people were impacted.
- With MFA enabled on the Citrix remote access, the attack probably doesn't happen.
- They paid the $22 million, but the hackers still leaked a lot of data.
- Change Healthcare processes 15 billion medical claims per year.
- Serves 900,000 physicians, 33,000 pharmacies and 5,500 hospitals.
- Direct cost estimated at $870 million.

CDK Cyberattack

June 18, 2024

- BlackSuit ties to Russia group Royal.
- Compromised VPN was likely the entry point.
- Interesting that BlackSuit bought access from an Initial Access Broker (IAB).
- Ransom of $10-50 million was demanded.
- Not confirmed, but there is speculation $25 million was paid to help restore.

What did we learn from this?

- A new Russian group was likely.
- More data was stolen.
- There were 15,000 dealerships impacted by CDK for up to two weeks.
- MFA enabled on VPN might have kept this from happening.
- Not confirmed that they paid 387 bitcoins worth approximately $25 million.
- There was a second attack and escalation of ransom to $50 million.
- Restoration was slow.
- Total loss is thought to be, at minimum, the $25 million in ransom. Nothing else is publicly known.

What's Happening This Year?

- NYC Sim Card Network
  - 300 Co-located SIM Servers; 100,000 SIM Cards
  - "In addition to carrying out anonymous telephonic threats, these devices could be used to conduct a wide range of telecommunications attacks. This includes disabling cell phone towers, enabling denial of services attacks and facilitating anonymous, encrypted communication between potential threat actors and criminal enterprises.

    While forensic examination of these devices is ongoing, early analysis indicates cellular communications between nation-state threat actors and individuals that are known to federal law enforcement."

What's Happening This Year?

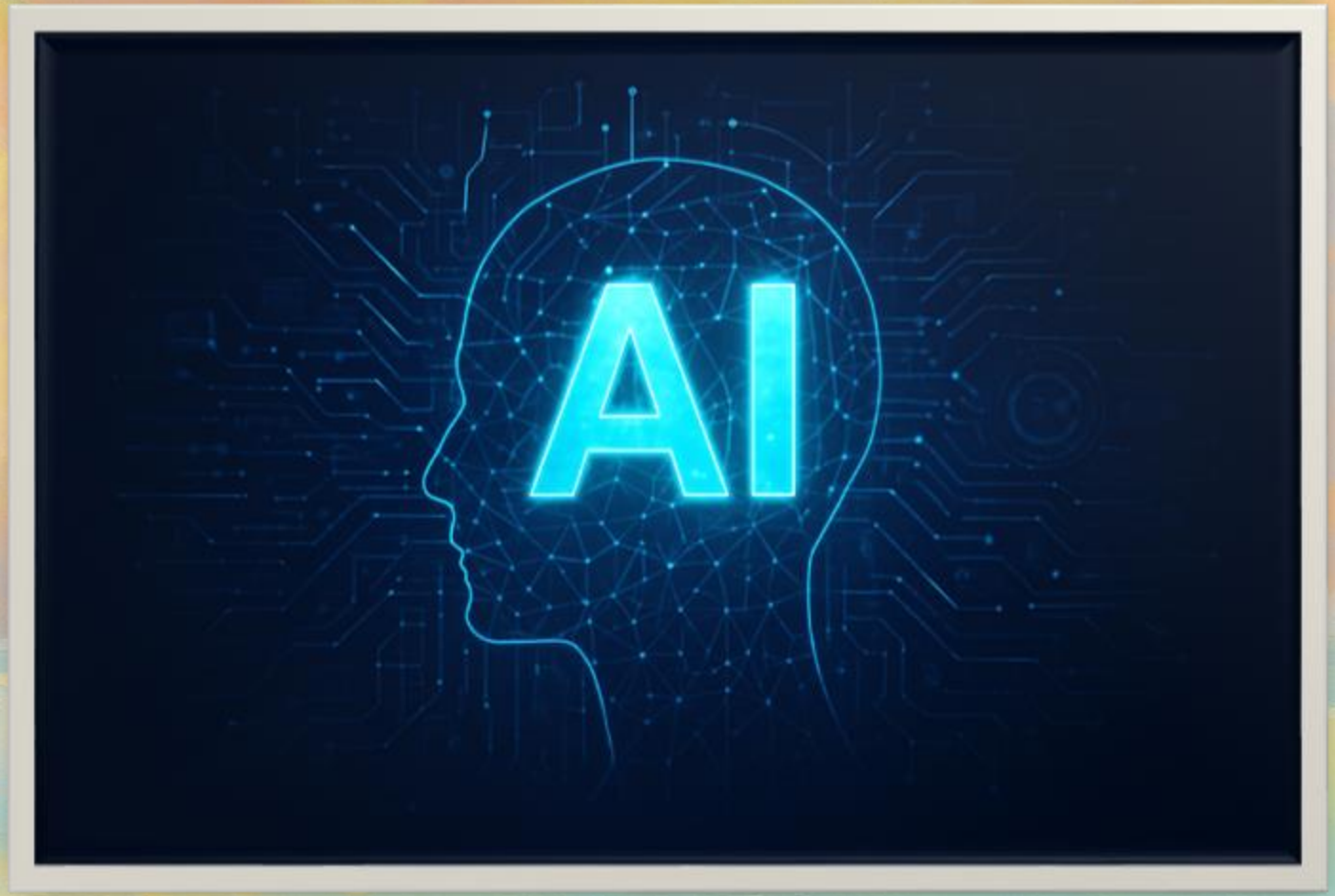
- Salesforce instances hit by Shiny Hunters.
- Qantas Airlines hit by Scattered Spider.
- Both groups unique – largely youngish (teens to 20s) white males in the US, UK and Canada.
- Vishing Attacks – Calling in impersonating IT support or calling in to get support from IT, getting passwords or MFA systems reset, then logging into the now stolen accounts.

Some people might be wondering why we went down this path of stories…

Top Takeaways from Others' Pain and Experiences

- Backups, backups, and then immutable backups.
- MFA on everything possible. If externally accessible with no MFA, you are running a huge risk. MFA has been quoted as stopping up to 99% of attacks.
- Most people might think MFA is on everything. Fairly certain some of the companies we covered thought so as well.
- Multilayer Security Approach – MFA is not enough; it is a start.
- Must have a scanning and patching program.
- Must have an EDR to detect and prevent unusual behavior.
- Must have email scanning and automated security protections.

No Cybersecurity Presentation Would be Complete Without AI



What to Focus on From a Security Perspective

- Your staff is using AI (and they should be using AI).
  - Make sure you have enforced MFA on AI.
  - Classify and label sensitive data (this is a BHAG).
  - Avoid feeding confidential or regulated data into public AI models.
    - A rule may be if you would not put the information on Facebook, don't put it in an open AI model.
    - There are safe ways of utilizing AI and confidential information. Copilot could be considered to be this.
  - Train employees on the risks of AI and explain the company AI policy.
  - Create an internal AI use policy. Define acceptable use, review cycles and incident response.
  - Commonsense might work as confidentiality and proprietary information handling should already be covered in policies.
  - Align with NIST AI framework and perform risk assessments.
  - Create an AI roadmap.

My One Use of AI Today – AI Recommends…

MINIMUM REQUIREMENTS FOR AI PROTECTION

Access Control & Authentication
- Enforce strong authentication (MFA, SSO)
- Restrict AI system access to authorized users

Data Protection & Privacy
- Classify and label sensitive data
- Encrypt data at rest and in transit

Monitoring & Logging
- Implement activity logging to AI interactions
- Continuously monitor for anomalies or misuse

Security Awareness Training
- Train employees on risks of AI
- Establish clear policies on what data can/cannot be shared

Vendor & Model Risk Management
- Vet AI vendors for compliance and security posture
- Use contracts defining data use, retention, and security responsibiities

Governance & Policies
- Create an internal AI use policy
- Define acceptable use, review cycles, and incident response steps

Technical Safeguards
- Use content filtering and red-teaming against AI models
- Implement guardralls for output validation and bias checks

What a Small to Medium-Sized Business' AI Roadmap Might Look Like

Step 1 (1-3 months)

- Define the problem you want AI to solve.
- Set measurable goals (e.g., reduce response times, improve forecasting accuracy).

Step 2 (1-3 months)

- Identify what data you already have.
- Clean and structure it.
- Fill gaps with external datasets or new collection methods.

Step 3 (1-2 months)

- For SMBs, this usually means adopting an existing AI SaaS tool rather than building from scratch.
- If custom development is needed, budget extra (3–6 months).

Step 4 (1-2 months)

- Pilot the AI solution with a small team or single workflow.
- Adjust processes to fit real-world needs.
- Collect user feedback.

Step 5 (1 month)

- Measure against your original metrics.
- If successful, expand across teams or departments.
- Establish ongoing monitoring, retraining and updates.

Regulations

All of these funding programs include cybersecurity requirements		
E-ACAM	**BEAD**	**REconnect5**
"reflect the NIST CSF" using either the CISA CPGs or the CIS Critical Security controls Included in 481 form	"reflects the latest version of the NIST CSF" Operational or ready to operationalize upon providing service	"must demonstrate, prior to the signing of the award agreement, a concerted effort to consider and address cybersecurity risks consistent with the cybersecurity performance goals for critical infrastructure and control systems"

NIST CSF

- Six Functions – Governance, Identify, Protect, Detect, Respond, Recover
- Start small and then build up. Consider the Small Business Profile.
- Governance – Put someone in charge, build policies, report back, supply chain.
- Identify – Vulnerability management, assess the effectiveness of the program, know your risks, communicate to your team.
- Protect – Restrict access, train employees, use MFA, scan/patch, backup, encryption.
- Detect – Monitor your network (or outsource), anti-malware.
- Respond – Incident management, test the IR process, include external stakeholders.
- Recover – Backup integrity checks, after-action reports, communicate.

Top Takeaways

- Remember that people are very often the weakest link.
  - Make sure you are training all your staff and testing them using SAT. C-level and accounting are high-value targets for phishing.
  - Make sure the culture supports making mistakes and how to report them.
  - Make sure you have MDR to monitor email 24x7, neutralize threats, rapid incident response and proactive threat hunting. There are many MDR needs and types, but BEC is still the number one attack vector by far.
- Make sure your backups are adequate for the risk you are willing to accept and that they are tested on a scheduled basis to be valid.
- Proper scanning and patching of your systems.
- Endpoint Detection and Response (EDR)
- Understand your encryption approach. Data at rest, in flight and in use.

Top Takeaways (continued)

- CISA has provided some great guidance recently that outlines:
  - Segmentation of IT and OT.
  - Enhanced logging. Security Information and Event Management (SIEM) might be hard to start with but start.
  - CISA has a lot of great documents and resources.
    - https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-month-toolkit
  - Link to CISA's Lessons Learned
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-266a
- Access Control List (ACL) and Geofencing. Anything you can do to reduce your attack surface is a great step.
- Review and update your Disaster Recovery Plan and Emergency Response Plan annually. If you do not have either of these, create them!

Top Takeaways (final)

- Have MFA enabled on all external services or cloud services that are possible.
- Review token expiration lifetime.
  - There are varying options on this and it is not easy or convenient. Think of this as if all your layers of defense failed, how long it would be before the token no longer works.
- The sad truth is, once they steal your token, they typically have everything they need until you revoke the token, or it expires.
- Lastly, use all defenses at your disposal. If one fails, hopefully the others do not.

Thank you for your time today!

If you would like to learn more about the CyberTech Committee, please contact anyone on the Committee, including the people listed below.

Derrick Owens – WTA

- derrick@w-t-a.org

Allan Reiter – Co-Chair

- areiter@nex-tech.com

Christian Hansen – Member

- Christian.Hansen@bakertilly.com