choose dupage

Beyond the Firewall

Cybersecurity Tales, Trends, and Tips

IMEC

Presented By:

WINSOR CONSULTING

Simple. Sincere. Secure. ***It's The Winsor Way.***

About Winsor

Winsor Consulting is a premier Managed Security Services Provider (MSSP) dedicated to helping businesses protect their data from cyber threats. Our team provides comprehensive security solutions tailored to the specific needs of each client, ensuring that their data is always secure.
With Winsor Consulting, businesses can trust our simple and sincere approach to cybersecurity, knowing that their sensitive information is protected against any security risks.

WINSOR CONSULTING
Simple. Sincere. Secure. ***It's The Winsor Way.***

Ryan Harvey

Director of Sales & Security Consultant

- Been with Winsor since 2016
- CMMC Registered Practitioner (RP)
- Performed 50+ cybersecurity assessments for small and midsized manufacturers since 2020 (Iowa, Illinois, and Arizona)

"I'm committed to providing top-tier services to our clients and am always looking for ways to improve our offerings. Whether it's conducting security audits, providing vulnerability assessments, or delivering incident response services, I'm always here to help businesses protect their sensitive data and systems."

RHARVEY@WINSORGROUP.COM

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

Tales From a Cybersecurity Company

Company One (2023 Incident)

Manufacturing company with around 200 employees:

- Only performing some file level backups of about 60% of their servers. No offsite backups were being performed.
- Running many outdated operating systems
- Flat network structure (no segmentation)
- No security toolsets in place
  - Had free anti virus
- No patching
- All end users were local administrators on their PCs
- No Cybersecurity Awareness Training for their employees
- No multifactor authentication in place

Technology spend was focused on “Operational Technology”

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

Company Two (2023 Incident)

- Transportation company with around 115 employees:
  - Actively engaged with a Managed Services Provider
  - The MSP was not performing regular patches
  - The MSP was “handling” backups for them… Still using tape backups
  - Only had a basic antivirus
  - Nothing for ‘firewall best practices
  - Had a flat network
  - All end users were local administrators on their PCs
  - No Cybersecurity Awareness Training for their employees
  - No multifactor authentication was deployed

Attack Vector for Company One

- Company One
  - One of the owners had clicked on a phishing email and typed in their credentials to a legitimate looking website
  - Owner was a domain admin, so the threat actor had unfettered access to the network and domain
  - The threat actor was in the environment for 89 days
  - Data was exfiltrated and the threat actors provided proof of data exfiltration
  - Threats were made to release financials, personal photos, and other data if ransom wasn’t paid

Attack Vector for Company Two

- Company Two
  - Their MSP had very poor Cybersecurity hygiene
  - The “primary tech” that supported the company had a weak password with no multifactor authentication. Same weak password was used on their backups
  - Accessed the environment via the “primary tech’s” credentials and had unfettered access and moved laterally throughout the environment
  - The threat actors were only in the environment for 15 days (very short time period) before executing their ransomware payload
  - Threatened of releasing the company’s data if the ransom wasn’t paid within 3 days. Ransom price was raised due to non-payment on their timeline.
  - After investigation occurred, it was confirmed that data was not exfiltrated

Financials: The Impact

- $550k+ in Ransom paid
- $200k+ in forensics fees
- $300k+ in recovery fees
- $100k+ in legal fees
- $120k+ in new hardware to upgrade
- $150k+ in new annual software for added security

- Cyber liability picks up a substantial portion on the ransom, legal, forensics, and recovery, however the companies were left with paying a fair amount out of pocket.

- 2 non-renewed cyber liability insurance policies

- Other fees and services to become eligible for new cyber liability

- These are the numbers that we are aware of… they also paid for credit monitoring for all of their employees, paid for a company to broker the ransomware payment, and paid for a call center service to answer employee questions and concerns.

Response: The Aftermath

After a ransomware attack, the aftermath can be difficult to navigate, here's what to expect in the aftermath of a ransomware attack, as well as best practices for recovery and prevention.

- Insurance company will assign you legal counsel as well as a forensics team
- They will also recommend using an IR Company from their "preferred vendors" list
- Determine the potential to recover all data from backups
- Negotiate with threat actors
- Decide on the ransom
- Confirm what data was exfiltrated
- Restore operations
- Communicate with employees
- Communicate with forensics
- Sanitize all systems
- Perform post-incident review
- Increase security weaknesses

What are the Trends?

Ransomware

The threat of ransomware attacks is on the rise, with new and sophisticated techniques being used to target businesses of all sizes.

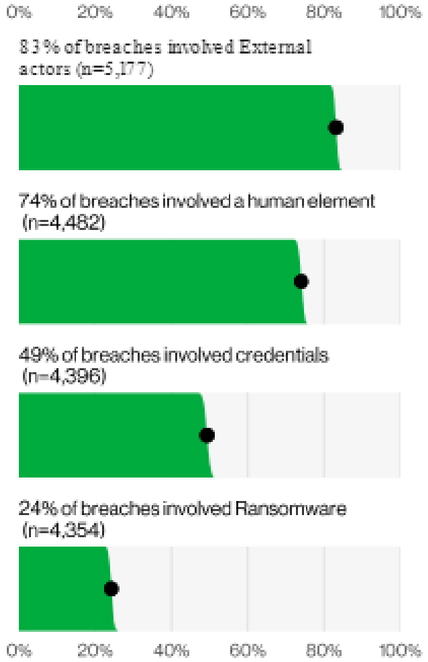


Figure 6. Select key enumerations

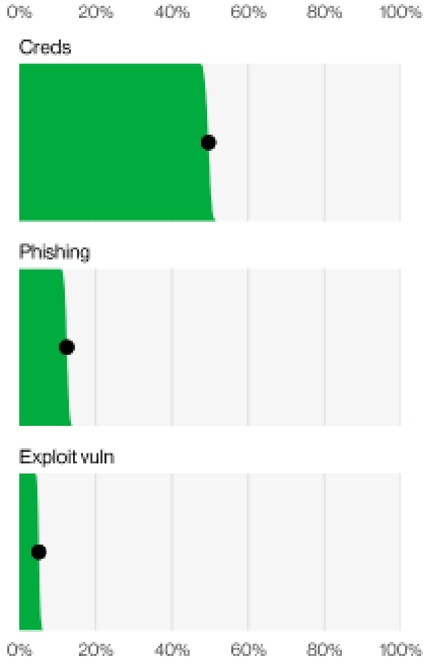


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

*Verizon's 2023 Data Breach Investigations Report

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

Cyber Liability Insurance

Cyber liability insurance is a type of insurance that helps protect businesses from the financial impact of cyber incidents such as data breaches, cyber-attacks, and cyber extortion.

Typical Policy Coverages:

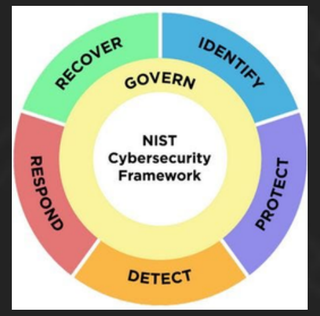
- Data recovery and restoration
- Loss of income due to downtime
- Legal fees and litigation expenses
- Notification costs
- Public relations and crisis management expenses

Have you seen Cyber Liability applications these days!?!?!

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

What Tips do we Have?

Where do we start?



1 Winsor suggests that you start with picking a cybersecurity framework that you want to follow as the "golden standard" within your organization.

- If you are within the Department of Defense Supply chain, you will need to follow NIST 800-171 (CMMC)
  - If you are not, we suggest following the NIST CSF or CIS Critical Security Controls (Top 18)
    - CIS will be easier to follow for the companies that don't have a very technical resource on staff

2 Based off which Cybersecurity framework you have chosen to follow, perform an assessment around all of the controls

3 Create a Plan of Actions & Milestones (POAM) based off of your findings

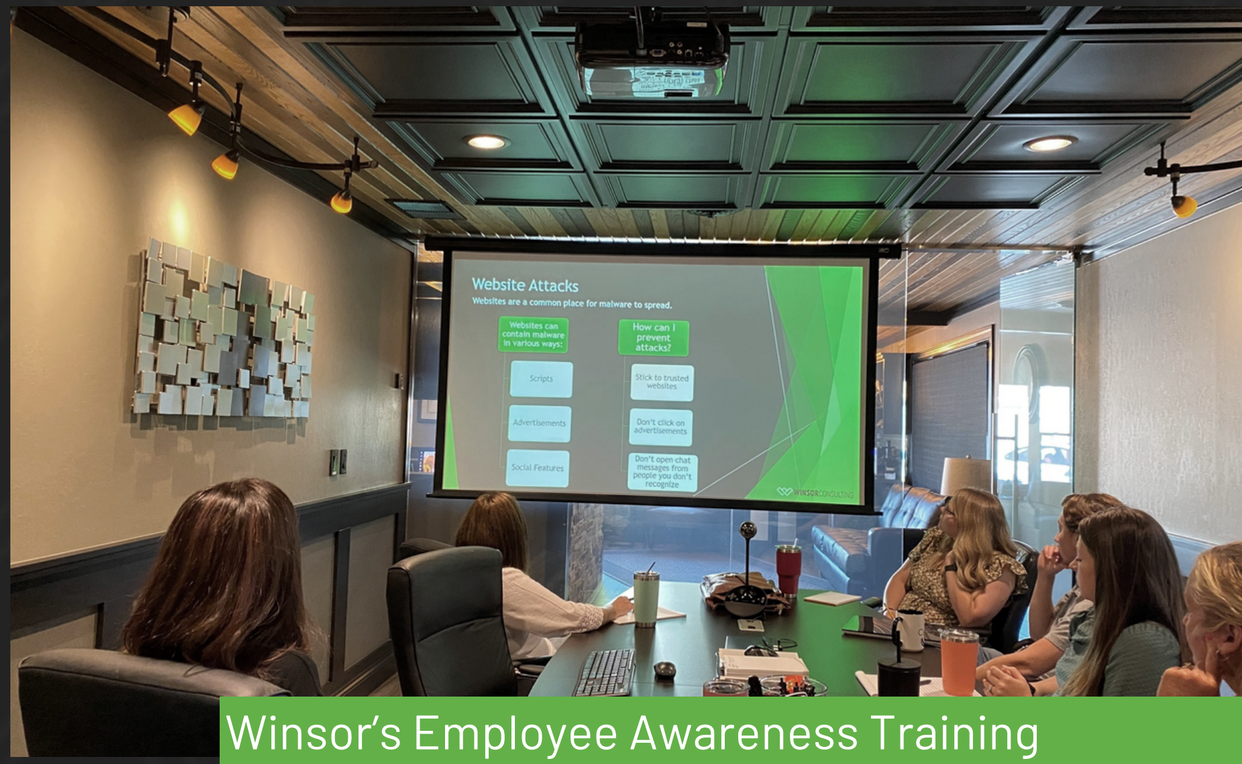
4 Prioritize ,you action list and just start working one item at a time

Even though Cybersecurity seems overwhelming, do not wait to start. Start small and make progress!

WINSOR CONSULTING
Simple. Sincere. Secure. *It's The Winsor Way.*

Prevention: It’s Not If, but When?

- Endpoint Detection & Response
- Managed Detection Response
- Security Awareness Training
- Regular Security Assessments
- Multifactor Authentication
- Enable SPF, DKIM, DMARC on email
- Develop patch management strategy
- Vulnerability management & remediation
- Privilege access management
- vLAN Segmentation
- Proper “offline” backups
- Security Information and Event Management (SIEM)
- Disaster Recovery and Incident Response Tabletop excercises



Winsor’s Employee Awareness Training

WINSORCONSULTING
Simple. Sincere. Secure. It’s The Winsor Way.

Ransomware: Do’s and Don’ts

- Activate your Incident Response Plan
- Isolate the infected machines from the network
- Consider the impact & extent of the attack
- Locate & verify offline backups
- Contact your cyber liability insurance
- Contact your attorney
- Contact the FBI

- Panic
- Power down any IT infrastructure
- Have IT start remediation
- Immediately pay the ransom
- Nothing

In the event of a ransomware attack, it's important to know what steps to take and what mistakes to avoid.

WINSORCONSULTING
Simple. Sincere. Secure. It’s The Winsor Way.

Question: Your Internal IT & Your MSP/MSSP

- Access Controls: Ensure that only authorized individuals have access to sensitive data, systems, and networks.
- Password Policies: Inquire about the strength and complexity of password policies and whether multi-factor authentication is required for EVERYTHING externally facing.
- Incident Response: Ask about the process for detecting, responding, and recovering from security incidents, including the frequency and rigor of testing and updating the incident response plan.
- Training and Awareness: Inquire about the training and awareness programs for employees on how to identify and respond to security threats.
- Risk Management: Ask about the organization's risk management framework, including the identification and assessment of risks, and the implementation of controls to mitigate them.

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

Question: Your Internal IT & Your MSP/MSSP

- Third-party Management: Inquire about the procedures for assessing and monitoring the security of third-party vendors who have access to the organization's systems or data.
- Compliance: Ask about the measures in place to ensure compliance with relevant laws, regulations, and industry standards, such as PCI DSS or HIPAA.
- Disaster Recovery: Ask about the backup schedule, the recovery time objective & recovery point objective. Ask them when the last full Disaster Recovery test was.
- Vulnerability Management: Inquire about the process for identifying, prioritizing, and remediating vulnerabilities in the organization's systems and networks.

WINSORCONSULTING
Simple. Sincere. Secure. It's The Winsor Way.

Any Questions?

By taking a proactive approach to cybersecurity and implementing best practices like cyber liability insurance and working with the right partner, you can mitigate the risks of cyber-attacks and keep your business safe in an increasingly digital world.

Winsor is a third party resource for IMEC and always willing to answer questions!

Jordyn Shawhan will send out a copy of the slides and a recording of the presentation

If you have questions or want to take the next step to cybersecurity peace of mind, make sure to reach out to your local IMEC Regional Manager or Camryn Tunney

ctunney@imec.org

WINSOR CONSULTING
Simple. Sincere. Secure. It's The Winsor Way.