CYBERSECURITY

Safeguarding Your Operations: Key Cybersecurity Practices

WINSOR CONSULTING

RYAN HARVEY
SALES DIRECTOR

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

COMMON GAPS WE OFTEN SEE.

- **Buying security products (i.e. EDR, SIEM, Backup Software, Firewall, etc) but don't properly configure or manage them**
- **Flat networks in place and don't think about cybersecurity on the shop floor**
- **Lack of Multi Factor Authentication or using it sparingly**
- **Lack of End User Cybersecurity Awareness training**
- **Not carrying Cyber Liability Insurance or minimal coverage**
- **Minimal attention paid to email security**

Many companies are content with their current IT status and assume everything is being taken care of. **Even the best IT teams should have their security posture verified.**

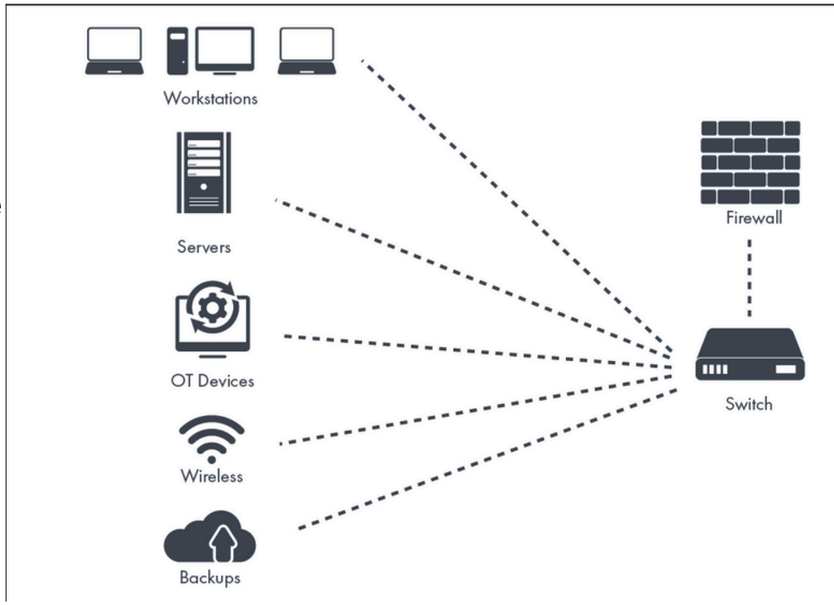
HOW OFTEN DO YOU THINK ABOUT OT? EXACTLY.

- Operational Technology (OT) environments are often connected to the internet and other internal networks, creating a security risk
- Outdated OT systems lack modern security features, making them easier targets for malicious actors
- The integration of various OT systems and devices can create complex environments that are difficult to secure and monitor, increasing the risk of breaches
- Vulnerabilities in the supply chain, such as compromised third-party software or hardware, can introduce threats to the OT environment
- Inadequate physical security measures can allow unauthorized personnel to access critical OT infrastructure, leading to potential sabotage or theft

WHY FLAT NETWORKS ARE RISKY FOR MANUFACTURING.

- Flat networks are where an environment is essentially on a single network
  - One breach can more easily spread across the entire network, impacting all systems and machines
  - Operational Technology is typically more outdated and unsupported, meaning that it is more succeptible to an attack
  - Once a threat actor gains access to a machine on the shop floor, the attack an easily spread to the servers, backups, office user's PCs
  - Flat networks make it difficult to identify and contain cyber threats quickly.

- We recommend segmenting your environment to shrink your attack surface



MULTI-FACTOR AUTHENTICATION & SINGLE SIGN ON:

- **Multi-Factor Authentication (MFA):** Uses two or more authentication methods (something you know, have, or are).
- **Password Vulnerabilities:** Threat actors can guess or steal passwords.
- **MFA on Key Systems:** Ensure MFA is on externally-facing systems (e.g., M365, Google Workspace, VPN).
- **Push Fatigue:** Users may approve false MFA requests due to fatigue.
- **Single Sign-On (SSO):** Simplifies authentication through a centralized platform (e.g., Microsoft Entra), improving security and reducing password reuse.
- **Cost-Effective Security:** Number matching MFA and SSO through Entra are included in many M365 plans, making these enhancements affordable for SMBs.

THE BIGGEST PROBLEM THAT FEW PEOPLE ARE TALKING ABOUT.

BUSINESS EMAIL COMPROMISES

BEC is a type of cybercrime where the threat actor uses email to trick someone into sending money or divulging sensitive company information

- Evilginx: Every company's archnemesis
- Monetary loss: A majority of BEC incidents will lead to a financial loss due to improper financial approvals and controls
- Insurance: Losses turned into your cyber liability provider will typically lead to rate increases
- Regulatory and Compliance Issues: BEC incidents can lead to non-compliance with data protection regulations, resulting in hefty fines and damage to the organization's reputation
- Supply Chain Vulnerabilities: Compromised email accounts can be used to exploit relationships with suppliers and partners, spreading the risk across the entire supply chain

- Create robust Conditional Access Policies within your M365 tenant (included in most M365 plans)
- Set up alerting from your M365 tenant to alert on items such as impossible travel, Outlook rules being created.
- Managed Detection Response for
- Establish strict procedures for approving financial transactions and train and....


0
DAYS WITHOUT
A CYBERSECURITY
INCIDENT.
0
WHEN YOU IMPLEMENT CYBERSECURITY MEASURES BUT DON'T TRAIN EMPLOYEES ON PREVENTING BUSINESS EMAIL COMPROMISES.

THE IMPORTANCE OF END USER CYBERSECURITY TRAINING.

Why? Because your end users are still your biggest threat!

- With advanced phishing tools being available to anyone for cheap or free, the constant barrage of phishing attempts will not be slowing down any time soon

- **AI & Cyber Threats:** AI complicates phishing, smishing, and vishing.
- **Protecting Assets**: Training safeguards data & systems, like safety training protects physical assets.
- **Preventing Human Error:** Most attacks exploit human mistakes—training reduces risks.
- **Ensuring Compliance:** Cybersecurity training helps meet regulations and avoid fines.
- **Maintaining Operations:** Cyberattacks can cause downtime, disrupting operations.
- **Adapting to Digital Threats:** More connected machinery means greater cybersecurity needs.

We recommend that you implement three end user training facets: weekly phishing simulations, monthly video training with quizzes, and yearly in-person training

Put a policy in place to hold individuals accountable for putting the company's data and money at risk.

WRITE THIS DOWN!

ZERO TRUST.

TRUSTED DEVICES.

- Zero trust is not a product or service, it is an approach in designing and implementing security principles
  - Always authenticate and authorize
  - Use least privilege (Just-In-Time and Just-Enough-Access concepts)
  - Assume breach
- Don’t trust anything or anyone
- Continuous monitoring and validation
- Least privilege
- Device access control
- Microsegmentation
- Lateral movement prevention
- Intune - only corp devices can access assets

MANUFACTURING
RANSOMWARE EVENT

- Illinois Manufacturing company
- The breach occurred when a leadership person clicked on a malicious email
- Every server was encrypted via ransomware and 85% of workstations were encrypted
- Had some backups that were only stored locally and not monitored and managed as they should be
- Running outdated operating systems
- No security toolsets in place and utilized free AV that did not have signature updates being applied
- Flat network
- **Spent a lot of money on the shop floor but not on securing the equipment and infrastructure that supports it**

COSTS THAT OCCURED

$200k+ in Ransomware paid

$100k+ in forensics fees

$200k+ in recovery fees

$50k+ in legal fees

$100k in new hardware to upgrade

Cyber liability picks up a substantial portion, but the companies were left with paying a fair amount out of pocket.

1nonrenewed cyber liability insurance policy

CYBER LIABILITY INSURANCE.

What factors control premium?

- Industry
- Revenue
- Type & Amount of Data
- Loss History
- IT Controls

DID YOU KNOW?

False statements could lead to your insurance claim being declined

Bare Minimum Controls

- MFA for all access
- Offsite (preferably offline) backups
- EDR
- Written plans for patches, updates, vulnerabilities
- Employee Cybersecurity Awareness training

More attractive requirements for underwriters

- Strong email filtering
- Privileged access management
- EOL software and hardware are segmented off the network with plans to replace
- IR & DR plans

What are underwriters looking for now

- Password Management
- SIEM
- DLP
- Following a security framework
- Maintain 24/7 SOC

WHAT CAN MANUFACTURERS DO?

- More companies need to perform periodic security assessments
  - Whether you have internal or outsourced IT
  - Consider continuous vulnerability monitoring
- Talk to your team about how you're using MFA (if at all)
- Change the mindset on Cyber Awareness Training
  - Financially, it's just as important as any other training
- Ask questions, what are we doing to secure our email?

THANK YOU!

Josh Falco - IMEC
jfalco@imec.org

Ryan Harvey - Sales Director
rharvey@winsorgroup.com
(563) 362-5476