FABTECH CANADA

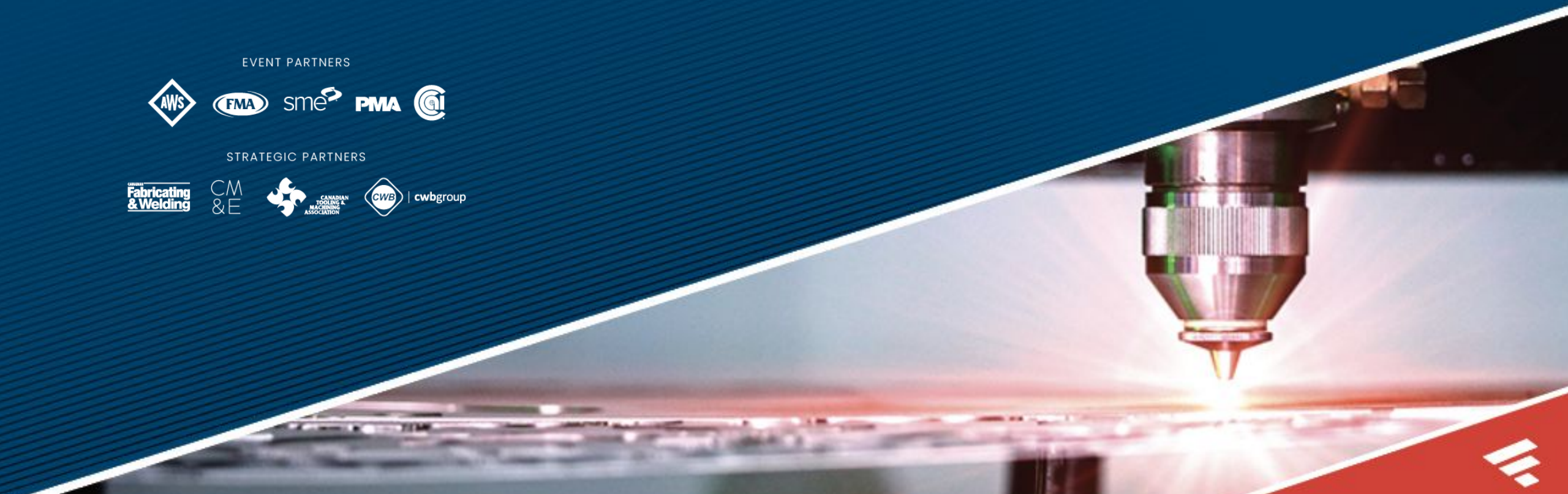
JUNE 14 - 16, 2022
TORONTO CONGRESS CENTRE

CANADA'S LARGEST METAL FORMING, FABRICATING, WELDING AND FINISHING EVENT

Building a Strong Cybersecurity Defense in an Increasingly Connected World

EVENT PARTNERS

STRATEGIC PARTNERS



Introduction

BitLyft Cybersecurity

Steve Mosley
VP of Sales
steve.mosley@bitlyft.com

CHARTER

Josh Patton
Principal Architect – Governance and Security
jpatton@charter.ca

FABTECH CANADA

Presentation Outline

1. Why Do Manufacturers Need to Prioritize Cybersecurity?
2. Why a Layered Approach is Needed
3. Why People and Resources are Still Needed for Good Security Posture
4. How Much Money Should My Company Spend on Cybersecurity?
5. Questions

FABTECH CANADA

Part 1

Why Do Manufacturers Need to Prioritize Cybersecurity?

FABTECH CANADA

4 Reasons a Good Cybersecurity Posture is Critical for Manufacturers

- Industry 4.0/Smart Manufacturing and IoT Connectivity
- External Factors
- Increasing Threats
- Cost of Downtime

FABTECH CANADA

1.) Industry 4.0/Smart Manufacturing and IoT Connectivity

FABTECH CANADA

2.) Compliance Requirements

(Government or OEM/Customer Demands)

FABTECH CANADA

3.) Increasing Threats

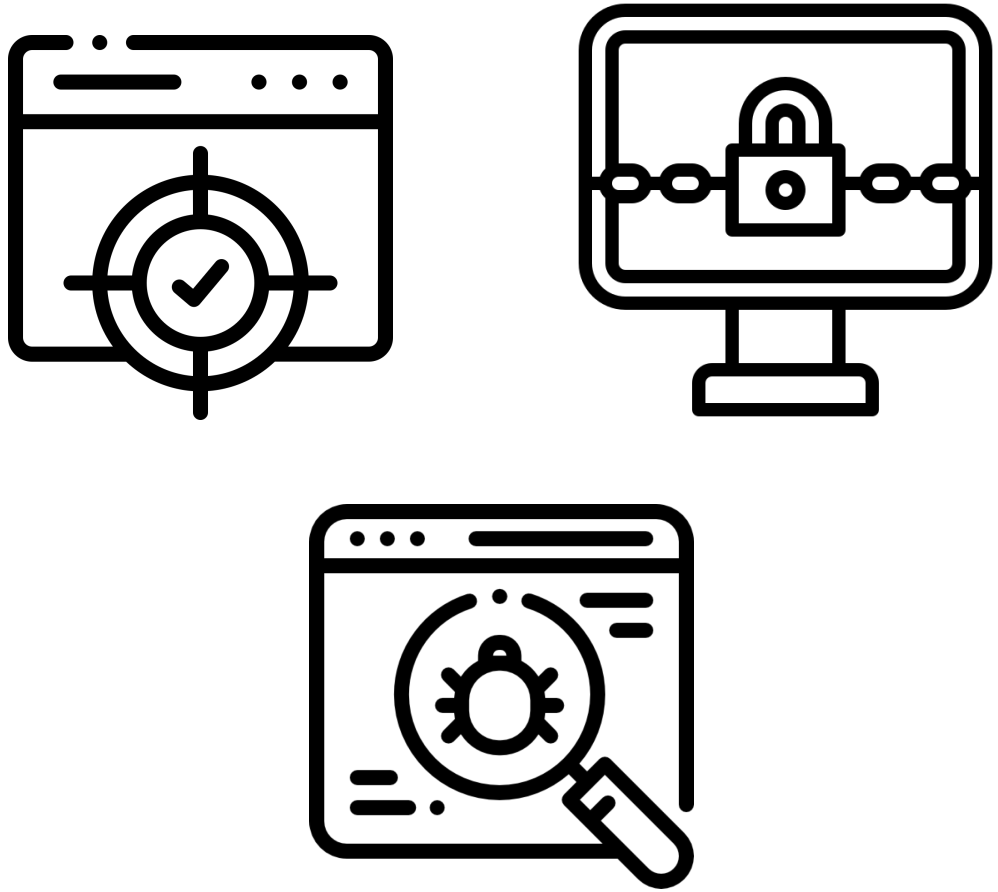
(Nation State Actors)

- By 2019, the manufacturing sector reached the Top 10 status as the 8th most targeted industry by cyber attackers.
- The problem exploded in 2020 when many companies were forced to depend almost entirely on remote workers due to pandemic restrictions.
- The manufacturing industry moved from the 8th most targeted industry by cyber attackers to number 2, falling behind only finance and insurance.
- According to the 2021 Global Threat Intelligence Report (GTIR), this represents a 300% increase in a single year.

FABTECH CANADA

Top Threats Against Manufacturers

- Phishing/Social Engineering
- Ransomware
- Internal Breaches
- Equipment Sabotage
- IP Theft
- Supply Chain Attacks



FABTECH CANADA

Why Are So Many Manufacturers Underprotected?

- Too many disparate solutions (No one knows where to start and which solutions are best/work together)
- Lack of resources and prioritization
- “It won’t happen to me” syndrome

FABTECH CANADA


Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
ICS + OT
Network Analysis & Forensics
Network Firewall
SASE
Deception
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB
TORONTO | 2022

Lack of Resources and Prioritization

- At the end of the day, who is responsible for risk management? Board/C-Suite, IT leadership? For smaller businesses who would that be (not always clear and not always a priority)
- Who runs the day to day when you are constrained on resources?
- When do you look at bringing on managed services?

FABTECH CANADA

Part 2:

Why a Layered Approach is Needed

FABTECH CANADA

Five Things You Should Be Able to Address

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

FABTECH CANADA

Top Tools/Solutions for a Layered Approach

Security Information Event Management (SIEM)	Endpoint Detection Response (EDR)
Password Vault	Single Sign On
Multi-Factor Authentication (MFA)	

Security Information Event Management (SIEM)

- Essential for good security posture for orgs of any size/across all verticals
- Essential to a layered approach and guarding against advanced threats
- Provides ability to look across your environment
- Allows you to make evidence based decisions for future cybersecurity spends/hires
- Essential for meeting compliance requirements which is needed for retaining and winning new customers

FABTECH CANADA

Endpoint Detection Response (EDR)

- Leverages machine learning to monitor user and system behavior to detect threats and ingest behavior for future threat detection - quarantines endpoint to remediate

Password Vault

- Best to leverage a password manager with an encrypted vault, audit capabilities and password generation features

FABTECH CANADA

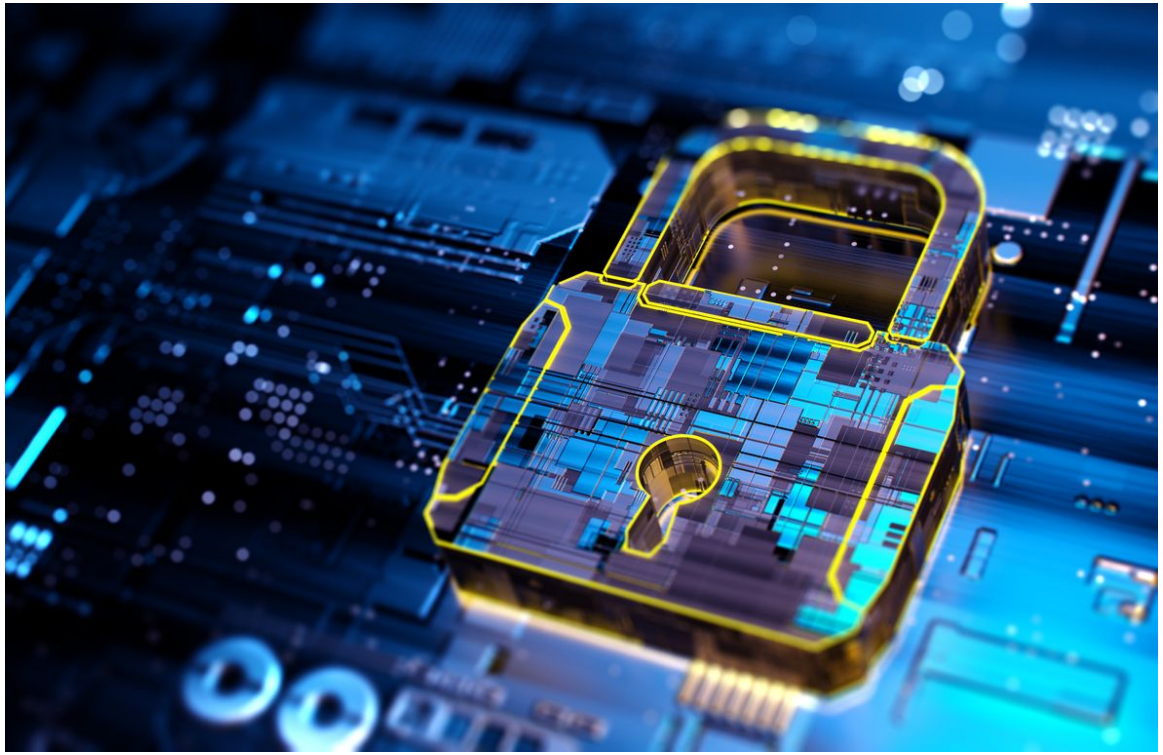
Single Sign-On (SSO)

- Safely controls access to company applications and systems
- Decreases attack surfaces
- Increases employee productivity

FABTECH CANADA

Multi-Factor Authentication (MFA-2FA)

- Requires an extra layer of security to access company systems and apps
  - Something you know
  - Something you are
  - Something you have



People and Resources are Still Needed for Good Security Posture

Five Questions You Should be Able to Answer	
• Do you have security policies and procedures in place?	• Do you have a security awareness training program for staff?
• Do you consistently audit configurations?	• Are you removing local admin rights from endpoints and servers?
• Are you monitoring security logs for the past 365 days?	

FABTECH CANADA

What's the Difference?

Managed Detection Response (MDR)	Security Operations Center (SOC)	Security Operations Center as a Service (SoCaaS)
• EDR • SIEM • Network traffic analysis • User and Entity Behavior Analytics (UEBA) • Asset discovery • Vulnerability management • Intrusion detection • Cloud vulnerability	• Internal hub of cybersecurity operations for your company • Organization maintains fulls control	• External company manages your internal security • Partners with existing IT staff to learn about your company's technology fingerprint • Manages a variety of security products and services • More cost effective than managing your own SOC • 24/7 Monitoring

Top 10 Questions You Need to Ask Any Service Provider

- What are your software requirements?
- How many people will be assigned to our organization?
- What happens when our contract is up for renewal?
- Do you have experience in our industry?
- How many clients are your analysts overseeing?
- How often and what does communication look like?
- How will you make a difference that we couldn't do on our own?
- Are you proactive or reactive?
- How will we know you are successful?
- Is your cybersecurity plan designed specifically for our organization?

FABTECH CANADA

Part 5

How Much Money Should My Company Spend on Cybersecurity?

FABTECH
CANADA

The Cost of Cybersecurity

- The cost to do nothing should be considered an essential business expense
- Automation and security AI saved companies up to $3.81 million
- A zero-trust approach reduced costs related to a data breach by up to $1.76 million

FABTECH CANADA

Budget Recommendation Example

ACME ORGANIZATION	
Gross Revenue	**$250M**
IT Budget	**$12.5M (5% of gross)**
Cybersecurity Budget (% of IT)	**$625,000 (5% of IT)**

Industry Benchmarks: % of IT budget spent on cybersecurity:*

- Software, Publishing & Internet Services: 9.5%*
- Retail & Wholesale: 5.3%*
- Higher Education: 3.6% (Times Higher Education)

*Source: Cybersecuritydive.com/Gartner

FABTECH CANADA

Closing Considerations

- Start with the most critical tools and build from there
- Automation and people is the future of security
- Know when you need to get outside help

Questions?