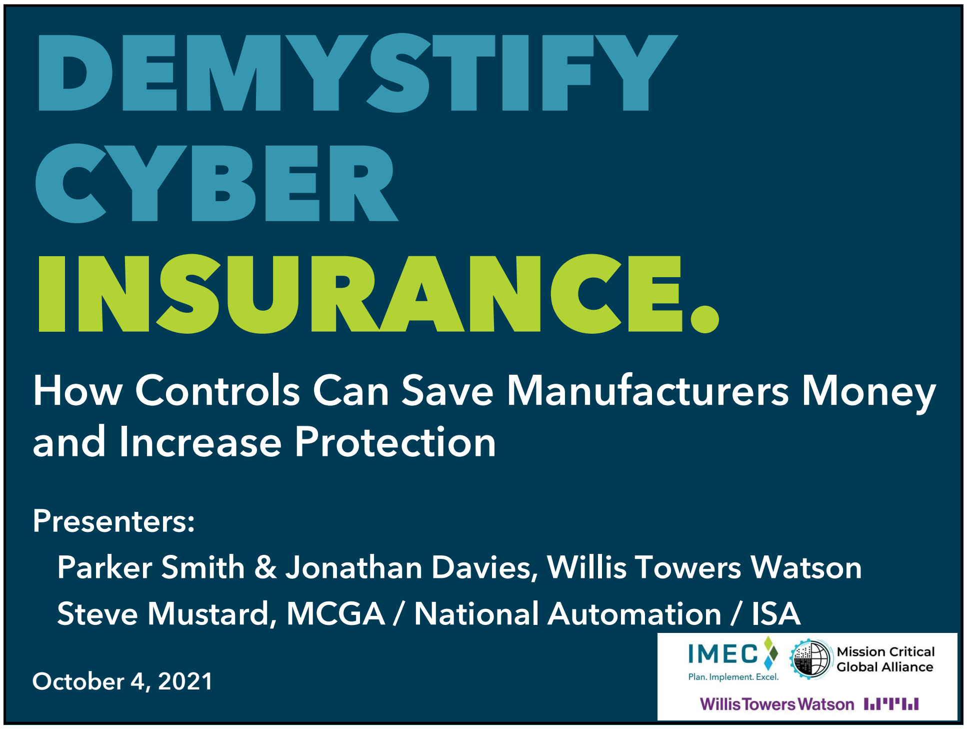


DEMYSTIFY CYBER INSURANCE.

How Controls Can Save Manufacturers Money and Increase Protection

Presenters:

Parker Smith & Jonathan Davies, Willis Towers Watson

Steve Mustard, MCGA / National Automation / ISA

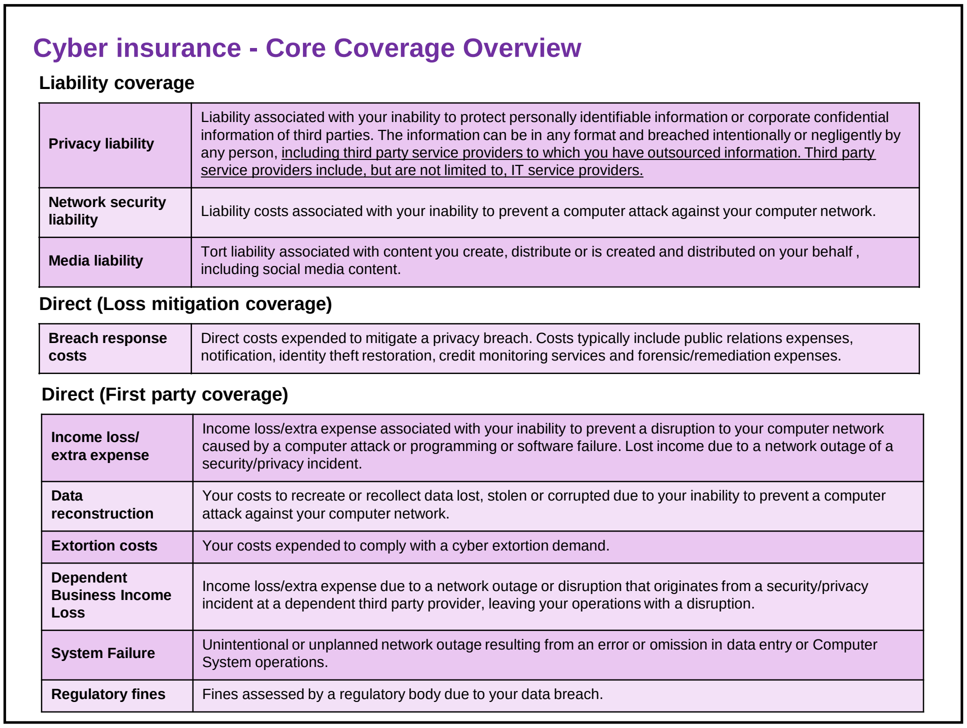
October 4, 2021

IMEC Plan. Implement. Excel.

Mission Critical Global Alliance

Willis Towers Watson

1



Cyber insurance - Core Coverage Overview

Liability coverage

Privacy liability	Liability associated with your inability to protect personally identifiable information or corporate confidential information of third parties. The information can be in any format and breached intentionally or negligently by any person, including third party service providers to which you have outsourced information. Third party service providers include, but are not limited to, IT service providers.
Network security liability	Liability costs associated with your inability to prevent a computer attack against your computer network.
Media liability	Tort liability associated with content you create, distribute or is created and distributed on your behalf , including social media content.

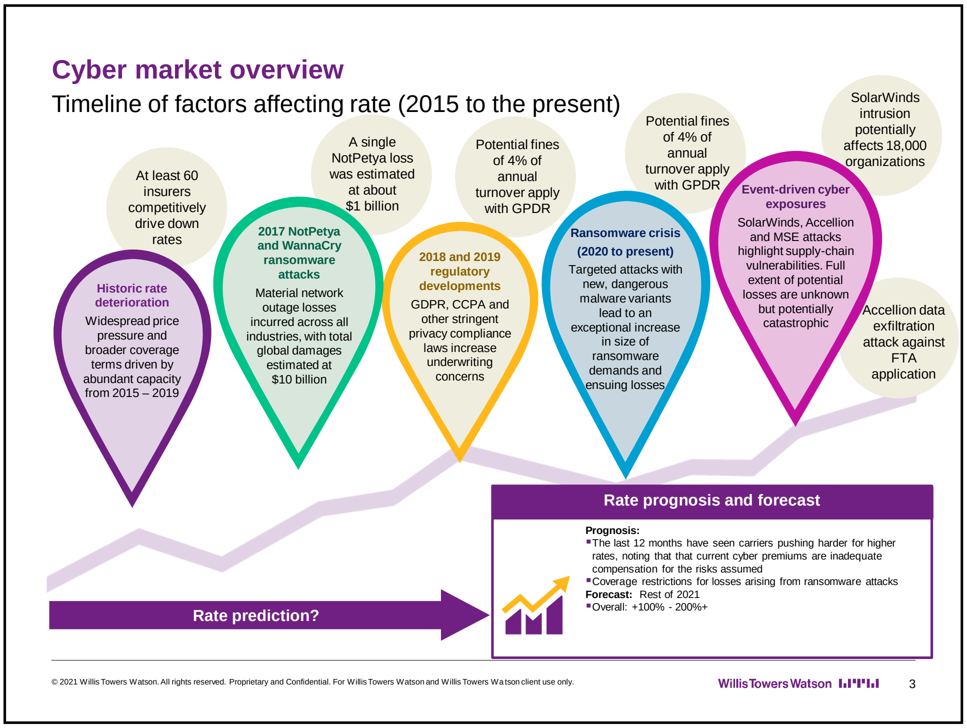
Direct (Loss mitigation coverage)

Breach response costs	Direct costs expended to mitigate a privacy breach. Costs typically include public relations expenses, notification, identity theft restoration, credit monitoring services and forensic/remediation expenses.

Direct (First party coverage)

Income loss/ extra expense	Income loss/extra expense associated with your inability to prevent a disruption to your computer network caused by a computer attack or programming or software failure. Lost income due to a network outage of a security/privacy incident.
Data reconstruction	Your costs to recreate or recollect data lost, stolen or corrupted due to your inability to prevent a computer attack against your computer network.
Extortion costs	Your costs expended to comply with a cyber extortion demand.
Dependent Business Income Loss	Income loss/extra expense due to a network outage or disruption that originates from a security/privacy incident at a dependent third party provider, leaving your operations with a disruption.
System Failure	Unintentional or unplanned network outage resulting from an error or omission in data entry or Computer System operations.
Regulatory fines	Fines assessed by a regulatory body due to your data breach.

2



Cyber market overview

Timeline of factors affecting rate (2015 to the present)

Historic rate deterioration
Widespread price pressure and broader coverage terms driven by abundant capacity from 2015 – 2019

At least 60 insurers competitively drive down rates

2017 NotPetya and WannaCry ransomware attacks
Material network outage losses incurred across all industries, with total global damages estimated at $10 billion

A single NotPetya loss was estimated at about $1 billion

2018 and 2019 regulatory developments
GDPR, CCPA and other stringent privacy compliance laws increase underwriting concerns

Potential fines of 4% of annual turnover apply with GPDR

Ransomware crisis (2020 to present)
Targeted attacks with new, dangerous malware variants lead to an exceptional increase in size of ransomware demands and ensuing losses

Potential fines of 4% of annual turnover apply with GPDR

Event-driven cyber exposures
SolarWinds, Accellion and MSE attacks highlight supply-chain vulnerabilities. Full extent of potential losses are unknown but potentially catastrophic

SolarWinds intrusion potentially affects 18,000 organizations

Accellion data exfiltration attack against FTA application

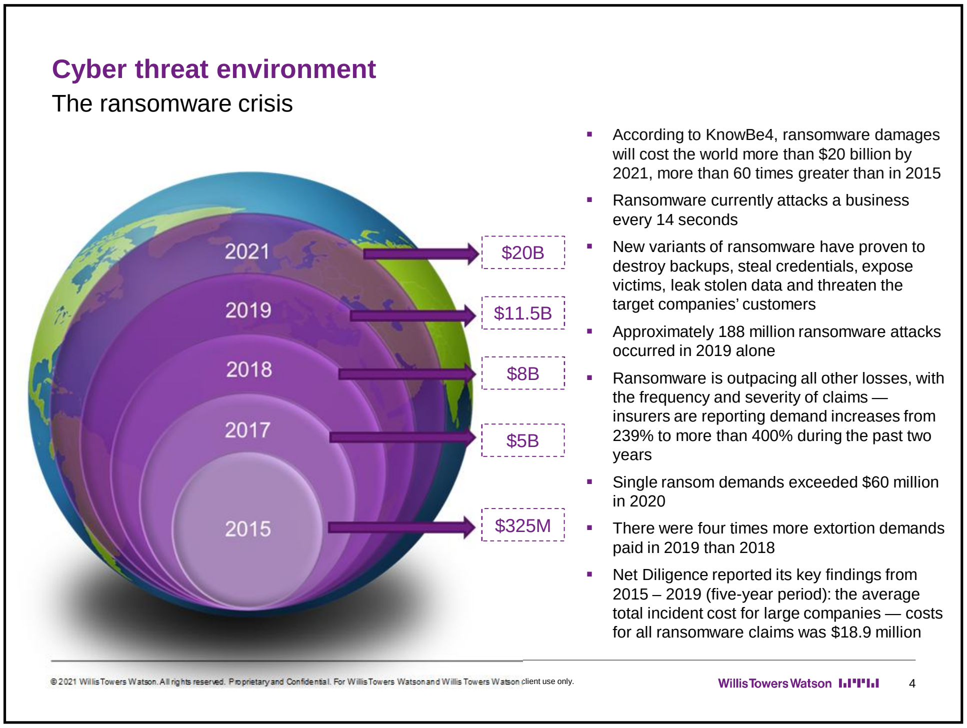
Rate prediction?

Rate prognosis and forecast

Prognosis:
- The last 12 months have seen carriers pushing harder for higher rates, noting that that current cyber premiums are inadequate compensation for the risks assumed
- Coverage restrictions for losses arising from ransomware attacks

Forecast: Rest of 2021
- Overall: +100% - 200%+

3

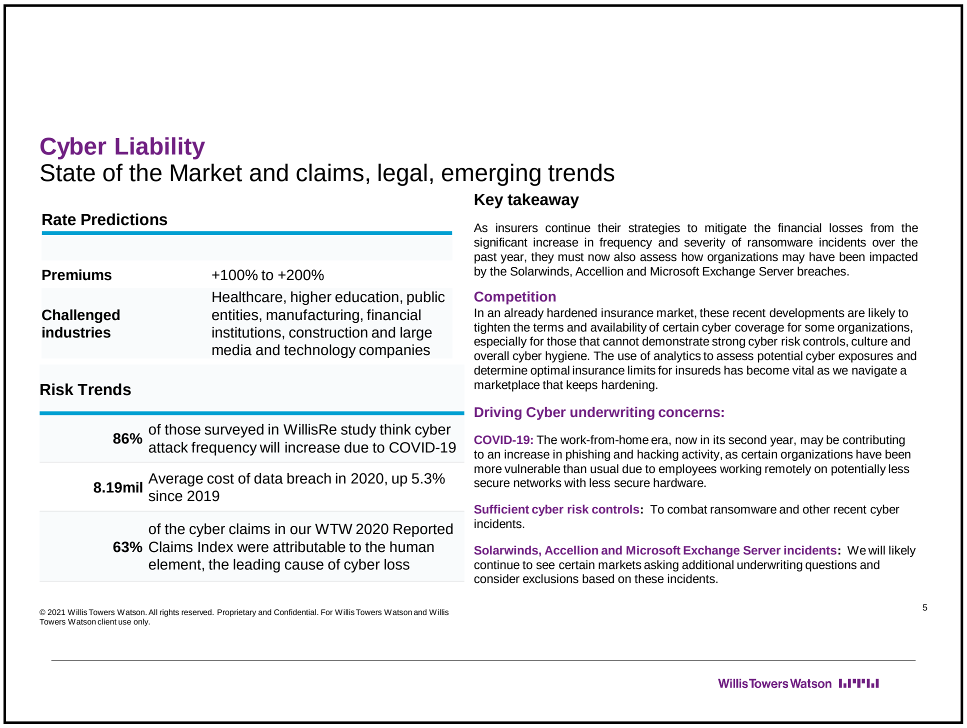


Cyber threat environment

The ransomware crisis

- According to KnowBe4, ransomware damages will cost the world more than $20 billion by 2021, more than 60 times greater than in 2015
- Ransomware currently attacks a business every 14 seconds
- New variants of ransomware have proven to destroy backups, steal credentials, expose victims, leak stolen data and threaten the target companies' customers
- Approximately 188 million ransomware attacks occurred in 2019 alone
- Ransomware is outpacing all other losses, with the frequency and severity of claims — insurers are reporting demand increases from 239% to more than 400% during the past two years
- Single ransom demands exceeded $60 million in 2020
- There were four times more extortion demands paid in 2019 than 2018
- Net Diligence reported its key findings from 2015 – 2019 (five-year period): the average total incident cost for large companies — costs for all ransomware claims was $18.9 million

4



Cyber Liability

State of the Market and claims, legal, emerging trends

Rate Predictions	
Premiums	+100% to +200%
Challenged industries	Healthcare, higher education, public entities, manufacturing, financial institutions, construction and large media and technology companies

Risk Trends	
86%	of those surveyed in WillisRe study think cyber attack frequency will increase due to COVID-19
8.19mil	Average cost of data breach in 2020, up 5.3% since 2019
63%	of the cyber claims in our WTW 2020 Reported Claims Index were attributable to the human element, the leading cause of cyber loss

Key takeaway

As insurers continue their strategies to mitigate the financial losses from the significant increase in frequency and severity of ransomware incidents over the past year, they must now also assess how organizations may have been impacted by the Solarwinds, Accellion and Microsoft Exchange Server breaches.

Competition

In an already hardened insurance market, these recent developments are likely to tighten the terms and availability of certain cyber coverage for some organizations, especially for those that cannot demonstrate strong cyber risk controls, culture and overall cyber hygiene. The use of analytics to assess potential cyber exposures and determine optimal insurance limits for insureds has become vital as we navigate a marketplace that keeps hardening.

Driving Cyber underwriting concerns:

COVID-19: The work-from-home era, now in its second year, may be contributing to an increase in phishing and hacking activity, as certain organizations have been more vulnerable than usual due to employees working remotely on potentially less secure networks with less secure hardware.

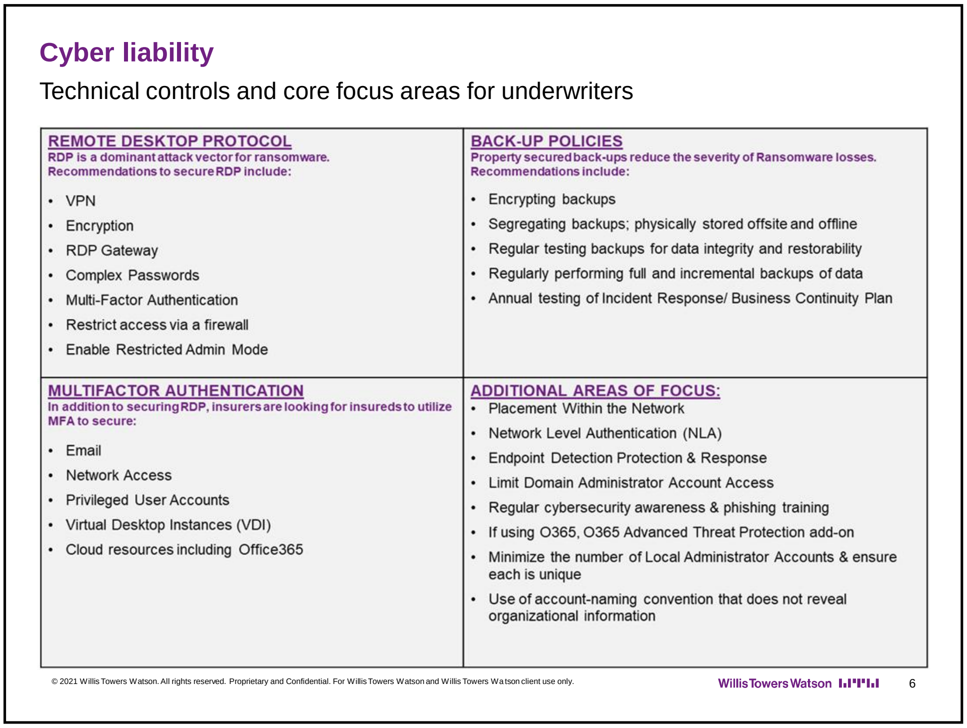
Sufficient cyber risk controls: To combat ransomware and other recent cyber incidents.

Solarwinds, Accellion and Microsoft Exchange Server incidents: We will likely continue to see certain markets asking additional underwriting questions and consider exclusions based on these incidents.

5

WillisTowersWatson

5



Cyber liability

Technical controls and core focus areas for underwriters

REMOTE DESKTOP PROTOCOL

RDP is a dominant attack vector for ransomware. Recommendations to secure RDP include:

- VPN
- Encryption
- RDP Gateway
- Complex Passwords
- Multi-Factor Authentication
- Restrict access via a firewall
- Enable Restricted Admin Mode

BACK-UP POLICIES

Property secured back-ups reduce the severity of Ransomware losses. Recommendations include:

- Encrypting backups
- Segregating backups; physically stored offsite and offline
- Regular testing backups for data integrity and restorability
- Regularly performing full and incremental backups of data
- Annual testing of Incident Response/ Business Continuity Plan

MULTIFACTOR AUTHENTICATION

In addition to securing RDP, insurers are looking for insureds to utilize MFA to secure:

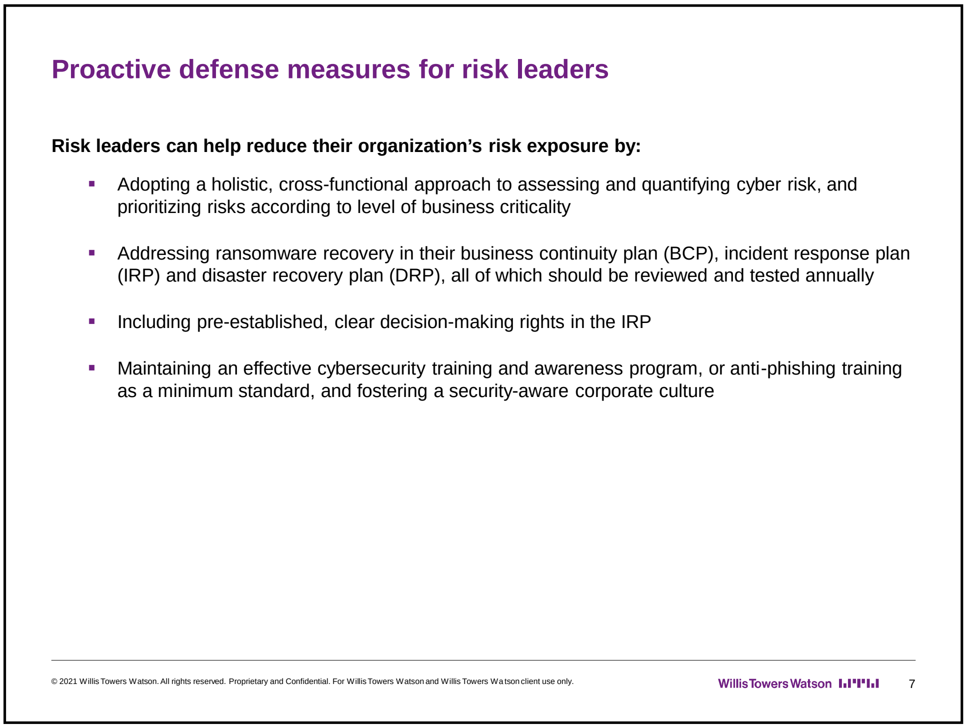
- Email
- Network Access
- Privileged User Accounts
- Virtual Desktop Instances (VDI)
- Cloud resources including Office365

ADDITIONAL AREAS OF FOCUS:

- Placement Within the Network
- Network Level Authentication (NLA)
- Endpoint Detection Protection & Response
- Limit Domain Administrator Account Access
- Regular cybersecurity awareness & phishing training
- If using O365, O365 Advanced Threat Protection add-on
- Minimize the number of Local Administrator Accounts & ensure each is unique
- Use of account-naming convention that does not reveal organizational information

WillisTowersWatson 6

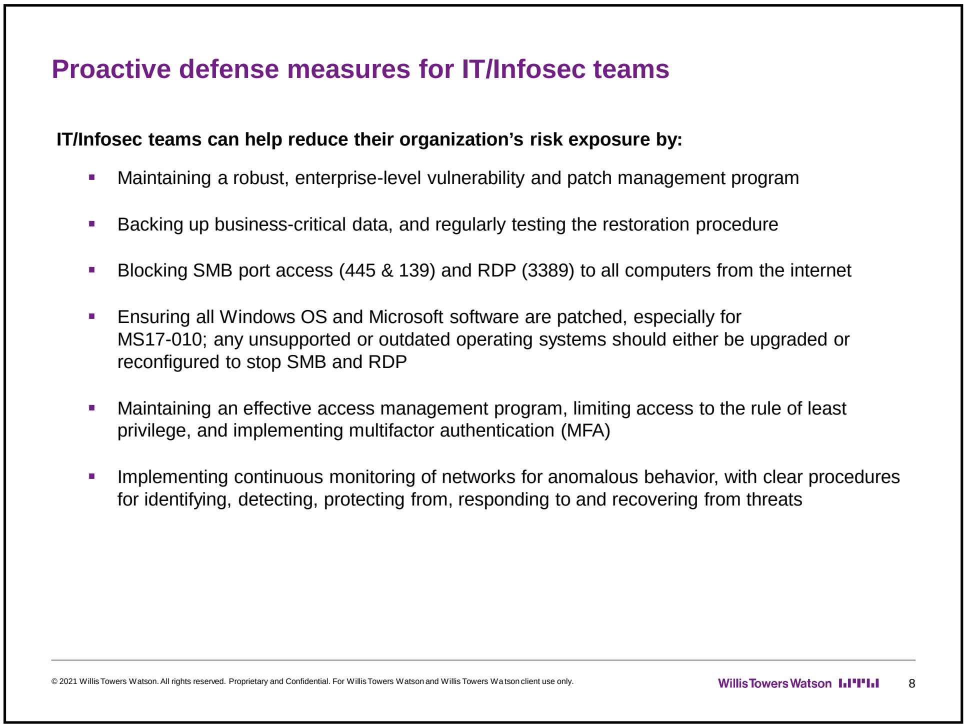
6



Proactive defense measures for risk leaders

Risk leaders can help reduce their organization’s risk exposure by:

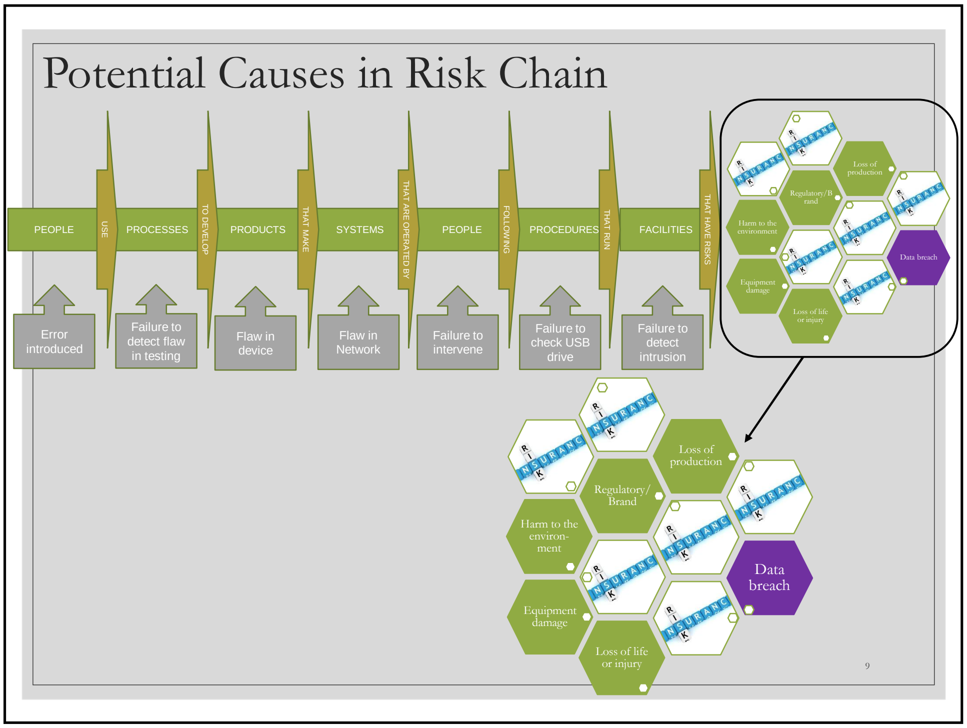
- Adopting a holistic, cross-functional approach to assessing and quantifying cyber risk, and prioritizing risks according to level of business criticality
- Addressing ransomware recovery in their business continuity plan (BCP), incident response plan (IRP) and disaster recovery plan (DRP), all of which should be reviewed and tested annually
- Including pre-established, clear decision-making rights in the IRP
- Maintaining an effective cybersecurity training and awareness program, or anti-phishing training as a minimum standard, and fostering a security-aware corporate culture



Proactive defense measures for IT/Infosec teams

IT/Infosec teams can help reduce their organization’s risk exposure by:

- Maintaining a robust, enterprise-level vulnerability and patch management program
- Backing up business-critical data, and regularly testing the restoration procedure
- Blocking SMB port access (445 & 139) and RDP (3389) to all computers from the internet
- Ensuring all Windows OS and Microsoft software are patched, especially for MS17-010; any unsupported or outdated operating systems should either be upgraded or reconfigured to stop SMB and RDP
- Maintaining an effective access management program, limiting access to the rule of least privilege, and implementing multifactor authentication (MFA)
- Implementing continuous monitoring of networks for anomalous behavior, with clear procedures for identifying, detecting, protecting from, responding to and recovering from threats



Potential Causes in Risk Chain

PEOPLE → USE → PROCESSES → TO DEVELOP → PRODUCTS → THAT MAKE → SYSTEMS → THAT ARE OPERATED BY → PEOPLE → FOLLOWING → PROCEDURES → THAT RUN → FACILITIES → THAT HAVE RISKS

Error introduced

Failure to detect flaw in testing

Flaw in device

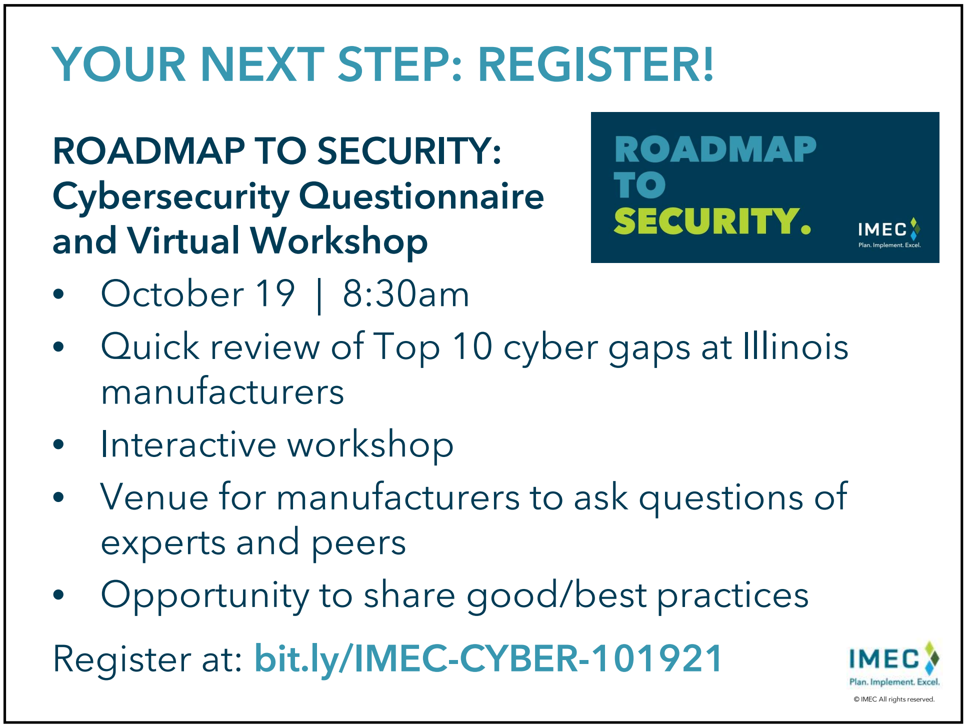
Flaw in Network

Failure to intervene

Failure to check USB drive

Failure to detect intrusion

9



YOUR NEXT STEP: REGISTER!

ROADMAP TO SECURITY: Cybersecurity Questionnaire and Virtual Workshop

ROADMAP TO SECURITY.
IMEC
Plan. Implement. Excel.

- October 19 | 8:30am
- Quick review of Top 10 cyber gaps at Illinois manufacturers
- Interactive workshop
- Venue for manufacturers to ask questions of experts and peers
- Opportunity to share good/best practices

Register at: **bit.ly/IMEC-CYBER-101921**

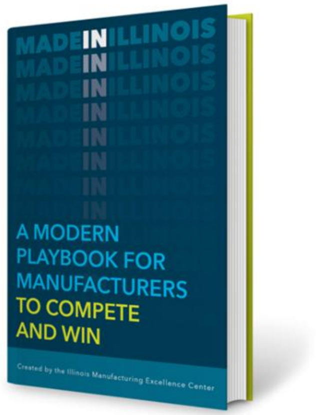
IMEC
Plan. Implement. Excel.

10

MADE IN ILLINOIS: A Modern Playbook for Manufacturers to Compete and Win

Chapter 6: Integrating Technology for Greater Process Innovation

- Mitigating Cyber Risk in a Virtual World


MADE IN ILLINOIS
A MODERN PLAYBOOK FOR MANUFACTURERS TO COMPETE AND WIN
Created by the Illinois Manufacturing Excellence Center

www.imec.org/made-in-illinois-playbook/

- Get your copy
- Strategy Guide
- Book Discussion Guide

11

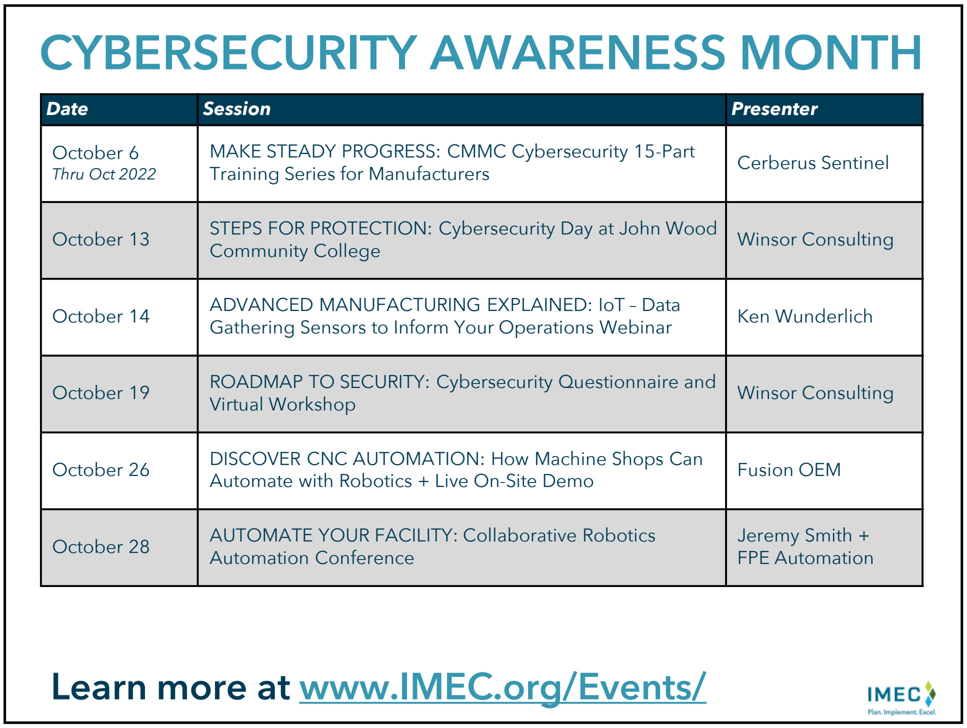
MAKE STEADY PROGRESS.

CMMC Cybersecurity Training for Manufacturers

- 23 companies currently registered
- 1st Wednesday per month through Oct. 2022
  - 3-hour monthly live, virtual training
  - Monthly homework guidance & IMEC check-in
  - Recording and resources for all 15 sessions
- Outlining the Department of Defense cybersecurity requirements
  - 1 set of controls / month
  - Prepare companies to confidently seek CMMC certification
- $3,500/company

Register: **bit.ly/IMEC-CMMC-Series-21-22**

12



CYBERSECURITY AWARENESS MONTH

Date	Session	Presenter
October 6 *Thru Oct 2022*	MAKE STEADY PROGRESS: CMMC Cybersecurity 15-Part Training Series for Manufacturers	Cerberus Sentinel
October 13	STEPS FOR PROTECTION: Cybersecurity Day at John Wood Community College	Winsor Consulting
October 14	ADVANCED MANUFACTURING EXPLAINED: IoT – Data Gathering Sensors to Inform Your Operations Webinar	Ken Wunderlich
October 19	ROADMAP TO SECURITY: Cybersecurity Questionnaire and Virtual Workshop	Winsor Consulting
October 26	DISCOVER CNC AUTOMATION: How Machine Shops Can Automate with Robotics + Live On-Site Demo	Fusion OEM
October 28	AUTOMATE YOUR FACILITY: Collaborative Robotics Automation Conference	Jeremy Smith + FPE Automation

Learn more at www.IMEC.org/Events/

IMEC
Plan. Implement. Excel.

13