LIVE WEBINAR

Manufacturing Cyber Security: Threats, Prevention & Response

AUGUST 12, 2025 / 11:00 AM CST

DAN ANFIELD
Account Executive
Travelers

BRETT SWIM
Managing Account Executive
Travelers

MELISSA DAYKIN CASSILL
Marketer, Risk
Cottingham & Butler

KATIE HENSLEY
Sales Executive, Risk
Cottingham & Butler

Before We Begin

- All attendees are in “LISTEN ONLY” mode.
- You can type in questions by using the question mark icon located on the top right portion of your screen.
- Q&A at the end of the webinar.
- Additional questions can be emailed to:

Kahensley@cottinghambutler.com or Mdaykincassill@cottinghambutler.com

This presentation is for general informational purposes only. This presentation is about coverages generally available in the marketplace and is not based specifically on the policies or products of Travelers Casualty and Surety Company of America and its property casualty affiliates ("Travelers"). This information does not amend, or otherwise affect, the terms, conditions, or coverages of any insurance policy issued by Travelers. This information is not a representation that coverage does or does not exist for any particular claim or loss under any such policy. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicable law. The availability of coverages referenced in this presentation may depend on underwriting qualifications and state regulations.

This presentation does not cover all possible cyber threats that may exist, does not identify all potential controls for those risks, and does not constitute legal advice. This presentation is not intended as advice to you or your insureds about specific risk control practices. It is not designed to be comprehensive, and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or advisor.

Agenda

- Why manufacturers are targeted
- Top threats and loss prevention
- Best practices
- Cyber insurance
- Travelers Cyber Risk Services
- Cyber claims process
- Claim scenarios

==========

!!! YOUR FILES HAVE BEEN ENCRYPTED !!!

==========

All of your important files — documents, photos, databases, and more — have been encrypted with a strong algorithm.You cannot access them. You cannot recover them without our help.

-Do NOT attempt to restore or modify files. Any such action may result in permanent data loss.

How to Recover Your Files:

To regain access, you must pay a ransom of 3.5 Bitcoin (BTC).

After payment, you will receive a decryption tool and instructions.

Payment Address: 1H4ck3dW4ll3tAddre55Xyz

You have 72 hours to comply. After that, your files will be permanently deleted and sensitive data may be leaked.

Free File Decryption:

To prove we can decrypt your files, you may send one file to: recover_support@protonmail.com

We will return it decrypted.

Do Not:

❌ Turn off your computer
❌ Contact law enforcement
❌ Attempt to remove this software

Any interference will result in immediate destruction of your data.

Why Now?

Rising Threats:

According to Travelers Q4 Cyber Threat Report:

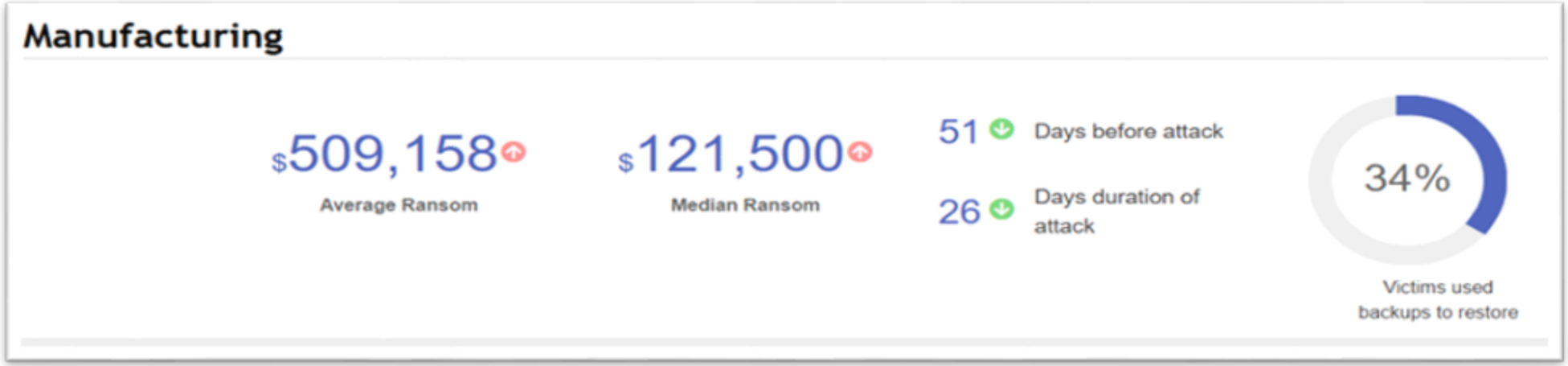
- The emergence of new ransomware groups surged **by 67% in 2024**, underscoring the growing sophistication and prevalence of cyber threats.
- There has been a shift towards more scalable and repeatable attack methods, making 2024 a pivotal year for cyber events.
- The number of ransomware attack victims posted on leak sites has **increased 72%** in the last two years alone.

The emergence of new ransomware groups surged by

↑67%

Ransomware attack victims posted on leak sites has increased by

↑72%



Targeting Manufacturing – Why?

- Manufacturing is the economic backbone making you a prime target. Ransomware can halt production impacting:
  - Finances (tight profit margins)
  - Contract obligations
  - Reputation
- Manufacturers hold valuable intellectual property, trade secrets, and operational data.
- Large workforces and complex operations increase the risk of accidental breaches.
- Outdated technology
- Older machines lack modern security features
- Poor integration with new tech creates vulnerabilities

Top threats:
Email compromise

Email Compromise

Web based email platforms are becoming more widely used

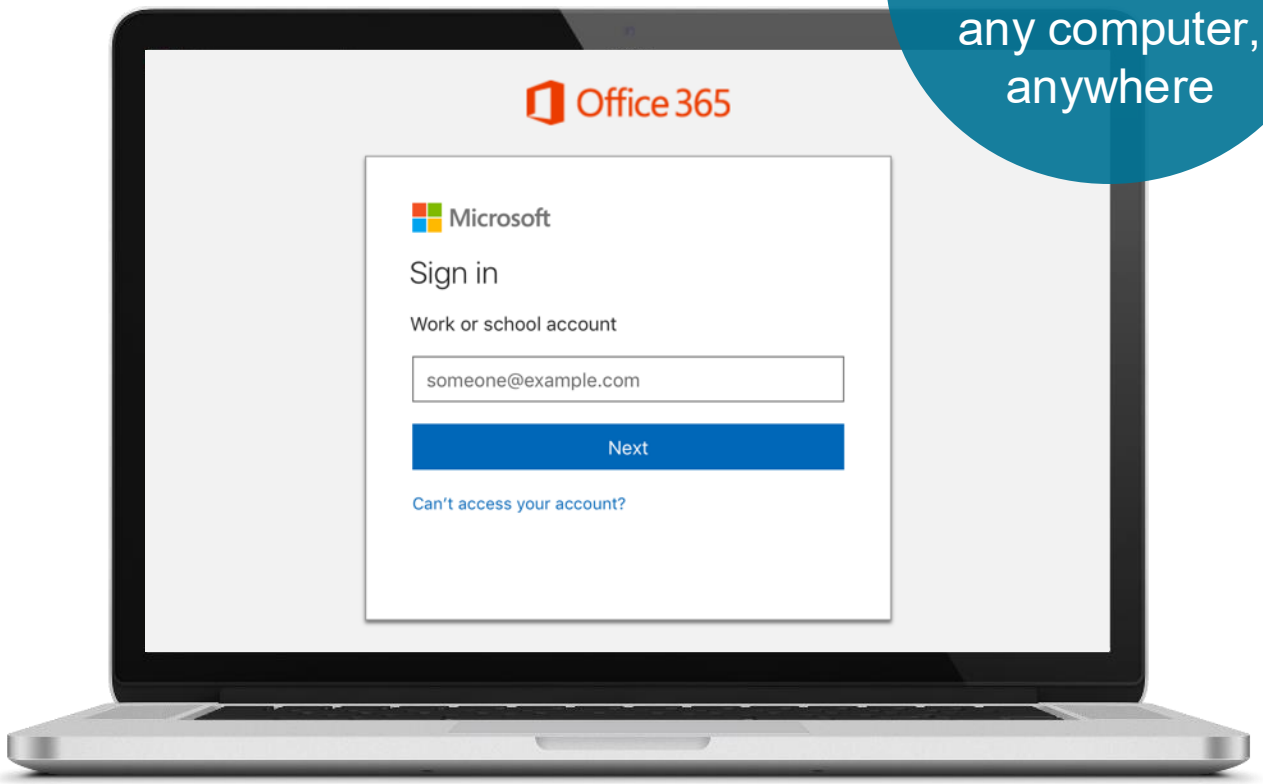
Once a fraudster has access to email, this access is used to perpetrate other crimes

- Social engineering fraud (SEF)
- Invoice manipulation
- Computer fraud
- Theft of personally identifiable information

In addition to any 1st party loss, Data Privacy laws require individuals whose confidential information was accessed within emails be notified

Notification costs | Forensic investigation | Legal fees

How Does Email Compromise Happen?



This login page is available from any computer, anywhere

Convenient for your workforce, but also convenient for cyber criminals

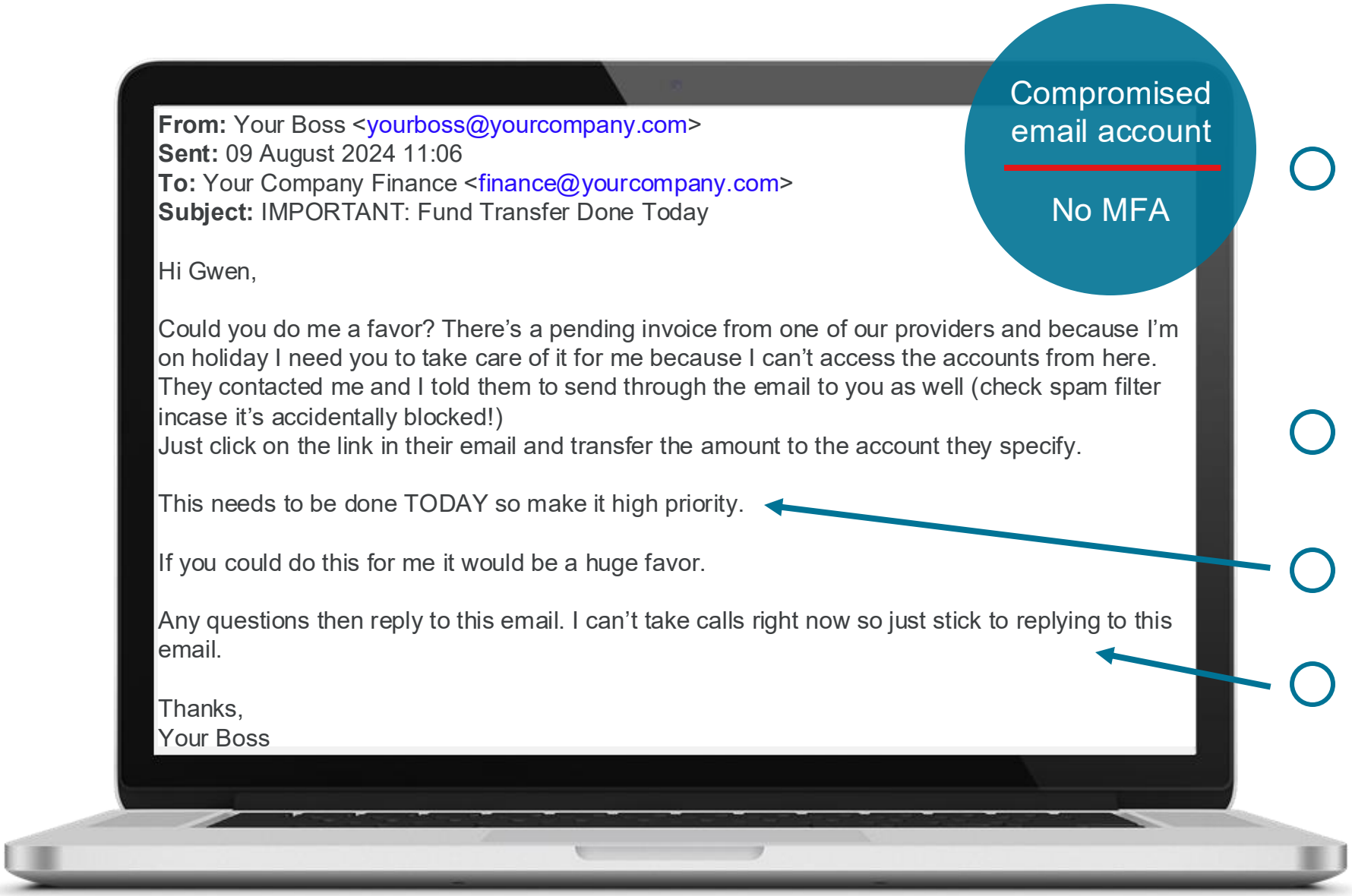
- If a username and password are the only requirements to access email, anyone that obtains that information has full access
- Threat actors (TA) have many sophisticated methods of obtaining this information

How Are Attacks Initiated?

Email initiated cyberattacks can start in a number of ways:

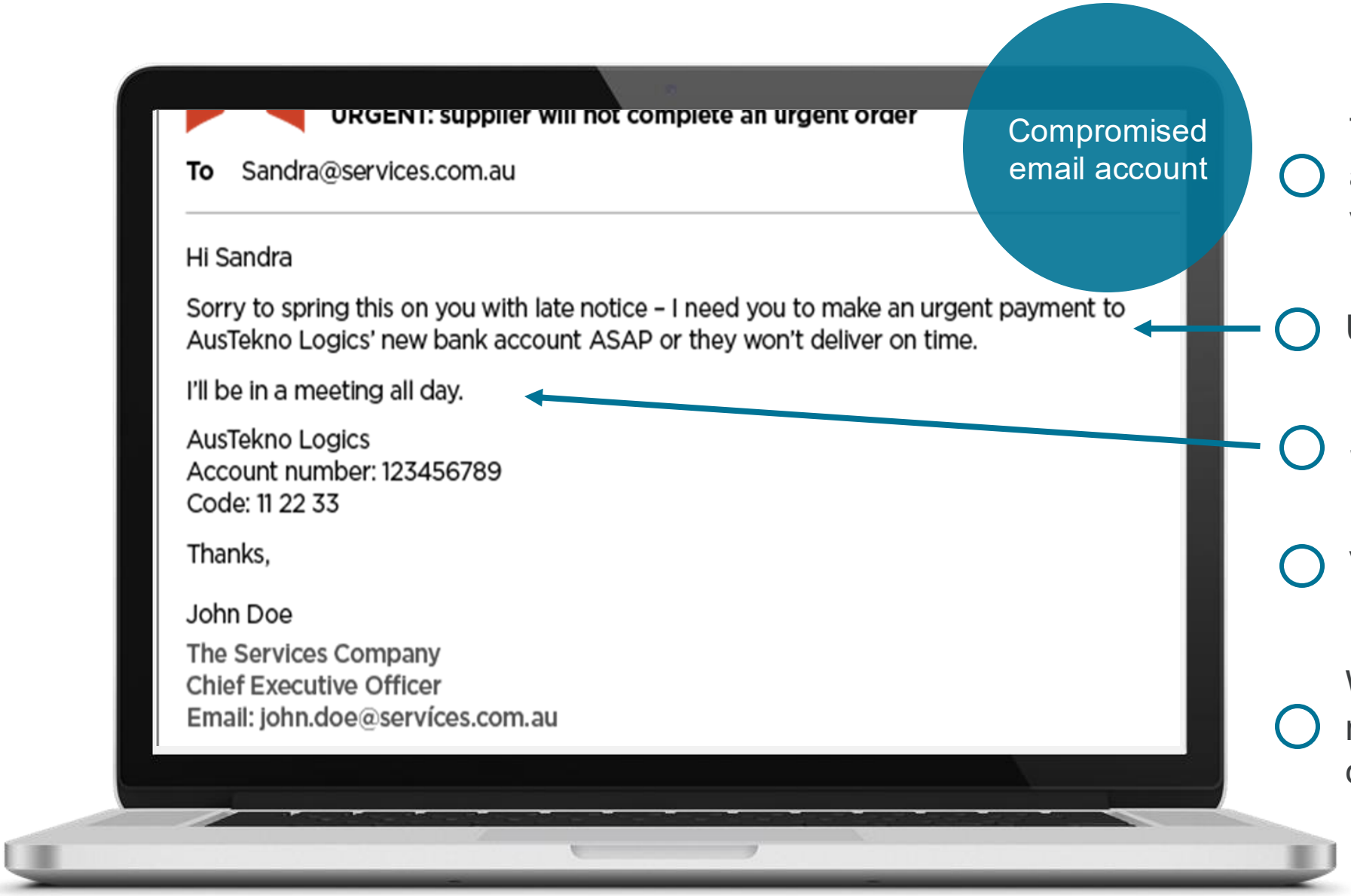
- Hackers alter settings for compromised account
- Monitor email traffic to understand organizational structure, speech nuances, etc. to inflict maximum damage
- Damage can come from accessing corporate intellectual property, databases, personnel files or customer and vendor information
- Hackers make things more difficult by covering their tracks and deleting activity logs
- Organizations vulnerable to these attacks tend to get hit repeatedly until vulnerability is addressed

Email Compromise: Employee to Employee



- TA targeting a subordinate—common tactic to pray on a person's willingness to please a superior
- Separate email sent with malicious link
- Urgent request—common tactic
- Sender can't be reached—common tactic

Email Compromise: Employee to Employee



Compromised email account

- TA acting as an employee to get another employee to change vendor bank information
- Urgent request
- Sender can't be reached
- Vendor probably IS owed money
- When vendor doesn't receive money, hack will likely be discovered

Email Compromise Loss Prevention

- Require multifactor authentication (MFA) for email and other web platforms
- Train staff to look for suspicious emails
- Promote culture of security awareness
- Don’t just delete suspect emails—report to IT
- Conduct phishing exercises on employees
- Be suspicious of requests to re-enter username and password
- Employ robust email filtering tools
- Block or alert new auto-forwarding rules

Top threats:
Ransomware

Ransomware:

Malicious software designed to block access to a computer system until money is paid

- New versions are sophisticated, encrypting data and backups, propagating quickly through systems
- Some versions involve element of data exfiltration
- Paying ransom is last resort, but becoming more common
- Smaller criminal groups can be troublesome to deal with: additional demands, key validity, etc.

Ransomware (Continues to Intensify)

More TAs and evolving variants

Attacker persistence

Ransomware as a Service (RaaS)

Evolving cryptocurrencies and valuation

Ramson demand amounts increasing and groups threatening to release data

Shared computer systems

Ransomware Loss Prevention

System security controls and maintenance

Secure remote connections

Disable Microsoft Office macros via group policy

MFA for remote access AND administrative access

Endpoint Protection and Response (EDR)

Patch critical vulnerabilities

Email filtering and external email warning is very important

Geo-blocking can help cut down on remote connections from IP addresses outside of region

Ransomware Loss Prevention

Backups

Segregated on the network or stored offsite, and tested regularly (by restoring from backups)

Threat intelligence sharing

Participate in groups such as InfraGard, US-CERT, SANS, etc.

Incident response/disaster recovery planning

- Tabletop exercises — know what to do before you're attacked
- Engage with forensic firms with knowledge of hacker groups
  - Will this group be able to deliver functioning encryption keys?
  - Negotiation tactics if payment of ransom is necessary

Best Practices

Separating Corporate (IT) and Manufacturing (OT) Networks

- Network Segmentation is Critical – Use firewalls/VLANs to isolate IT from OT environments
- Limit Access Paths – No direct IT-to-OT access; use secure jump servers or proxies
- Use MFA and Least Privilege – Especially for any access into OT systems
- Avoid Shared Systems – No shared AD, file servers, or credentials between IT and OT
- Monitor Separately – Deploy OT-specific monitoring tools and test segmentation regularly

Other Best Practices

- Multifactor authentication for email access, remote access, and access to administrative accounts (should also enforce strong password policies)
- Data protection- properly configured firewalls, data encryption, regular back ups using 3-2-1 rule
- Endpoint protection- EDR solution, frequent patching cadence
- Security awareness- training for all employees including phishing tests
- Incident response- disaster recovery and business continuity plan in place with regular testing
- Vendor management- security requirements for 3rd party vendors including contractual security obligations

Cyber Insurance

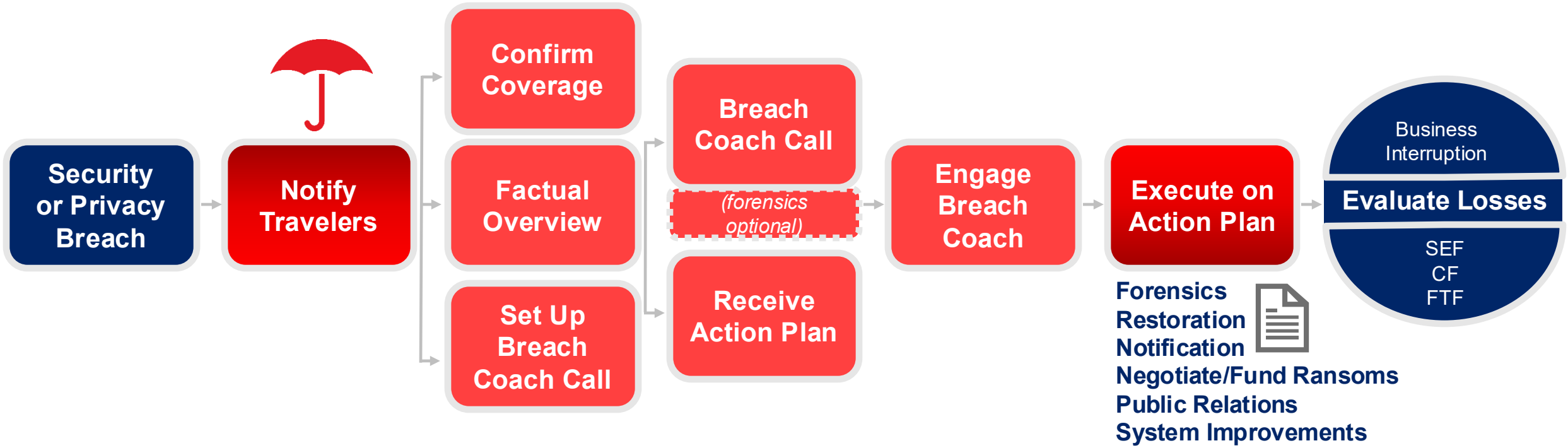
Four General Areas of Coverage

LIABILITY	BUSINESS LOSS	BREACH RESPONSE	CYBER CRIME
• Privacy & security • Media • Regulatory	• Business interruption • Dependent business interruption • System failure • Reputation harm	• Privacy breach notification • Computer & legal experts • Public relations • Cyber extortion • Data restoration	• Computer fraud • Funds transfer fraud • Social engineering fraud • Telecom fraud

Travelers Cyber Risk Services

- Cyber Risk Dashboard
- External perimeter scanning
- Personalized alerts for emerging cyber threats
- Continuous dark web monitoring
- Cyber expert security consultations
- Multifactor authentication implementation support
- Self- service risk assessment
- Employee security awareness training
- Discounted vendor rates
- Cyber newsletter and webinars

CyberRisk Breach Response Continuum



26

Cyber claim scenario

Computer Virus

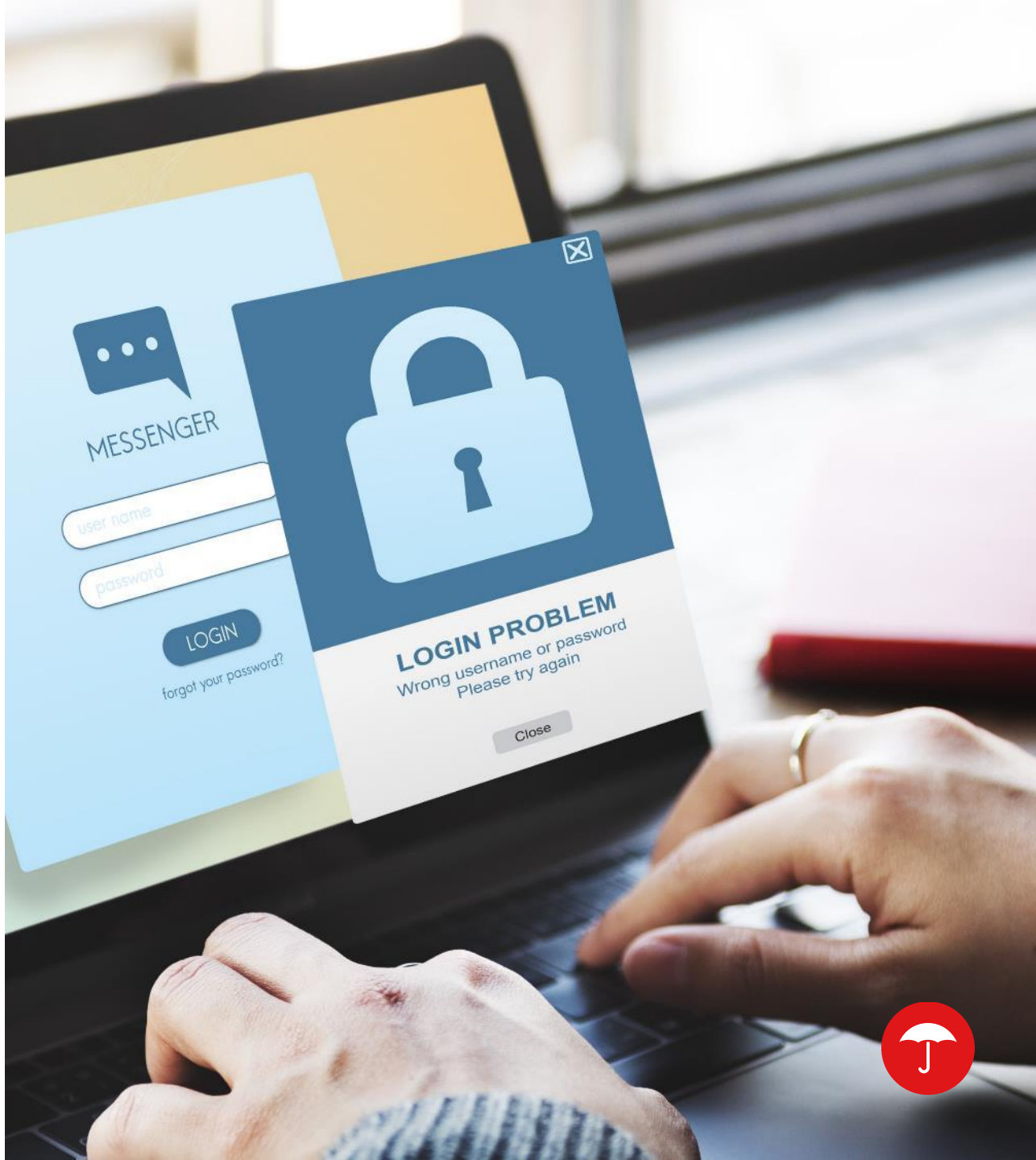
The server at a manufacturing plan with 100M in revenue was infected with an undetectable malware causing a 3-day shut-down of the production system. The manufacture immediately retained a computer forensic expert to investigate, incurred substantial costs associated with repairing and restoring its systems and suffered significant revenue loss from the shutdown. According to the NetDiligence Business Interruption Costs Calculator the estimated costs could be $821,000

Cyber claim scenario

Phishing Email Scam

An employee at a manufacturer opened a phishing email that infiltrated its centralized network, exposing names, addresses, Social Security numbers and financial information such as credit card and bank account numbers of 5,000 of its customers. A computer forensic investigator was hired and determined that Personally Identifiable Information (PII) was compromised. The manufacturer notified the affected customers, offered free credit monitoring for one year and hired a public relations firm in anticipation of bad publicity

because this was not the first time the manufacturer experienced a breach. Several states launched investigations and fines were imposed for the repeated failure to protect PII



Questions

Let’s Stay Connected!

Melissa Daykin Cassill
Marketer, Risk
Cottingham & Butler
mdaykincassill@cottinghambutler.com

Katie Hensley
Sales Executive, Risk
Cottingham & Butler
kahensley@cottinghambutler.com

SCAN THE QR CODE TO VISIT OUR WEBSITE

Follow Us @cottinghambutler | www.cottinghambutler.com