



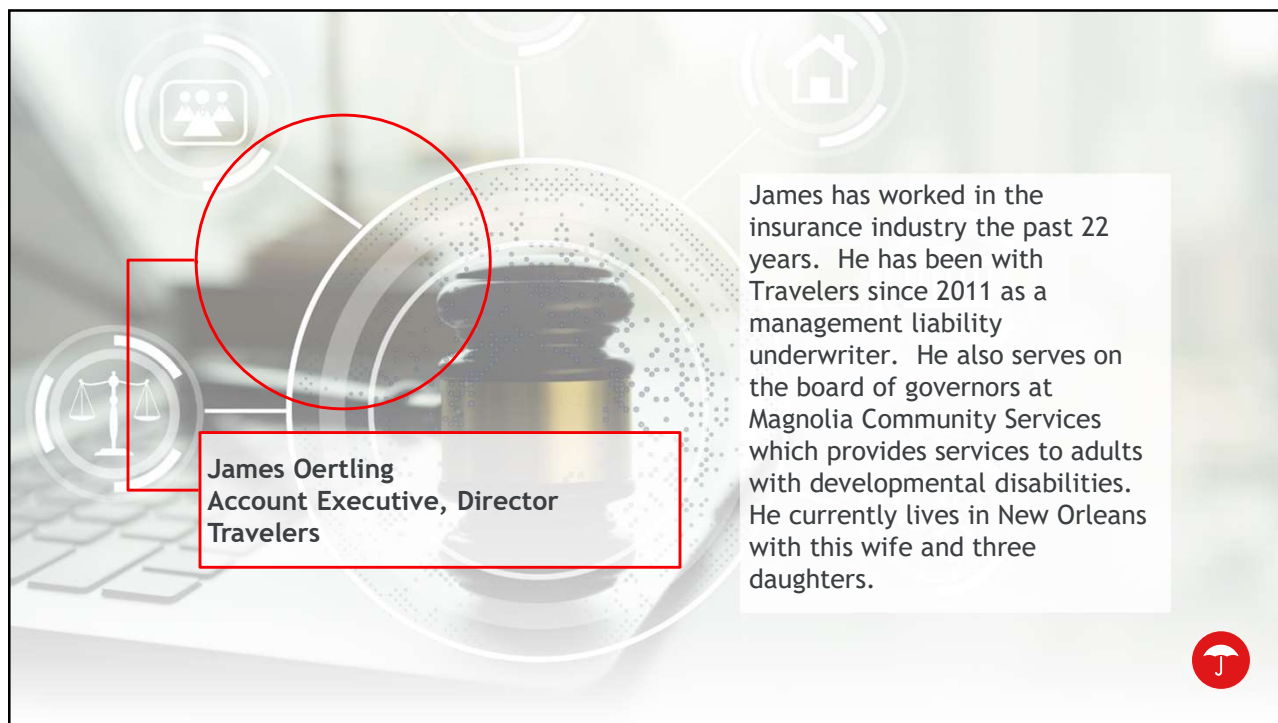
TRAVELERS^J

Cyber Threats, Loss Prevention and Claims

Continuing Education Presentation

James Oertling • Travelers Bond & Specialty Insurance • June 19, 2024

1



James Oertling
Account Executive, Director
Travelers

James has worked in the insurance industry the past 22 years. He has been with Travelers since 2011 as a management liability underwriter. He also serves on the board of governors at Magnolia Community Services which provides services to adults with developmental disabilities. He currently lives in New Orleans with this wife and three daughters.



2

Continuing education courses are intended to provide general information about the subjects covered and to help agents and brokers satisfy their professional licensing requirements. These courses are not intended as, nor do they constitute, legal or professional advice, nor are they an endorsement of any source cited, or information provided. Continuing education requirements may differ by state. Contact the applicable state licensing entity if you have questions regarding your professional licensing requirements.

Any examples or discussions of coverages are about coverages generally available in the marketplace, and are not based specifically on the policies or products of Travelers. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law.

Claims scenarios are based on actual claims, composites of actual claims, or hypothetical situations. Resolution amounts are approximations of both actual and anticipated losses and defense costs. Facts may have been changed to protect confidentiality. Any examples or discussions of claim handling or processes are for illustrative purposes only. Every claim is unique and must be evaluated on its own merits.



3



Agenda

- Top threats & loss prevention
 - Email compromise
 - Ransomware
 - Credential theft & failure to patch
- Important concepts
- By-the-numbers
- Cyber claim themes
- Cyber insurance



4

Top threats: Email compromise



5

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 e-mails be notified



Notification costs | Forensic investigation | Legal fees



6

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

7

How is login information obtained?

- Emails with malicious links or tainted attachments; may recommend password change
- Dark web acquisition of compromised emails addresses and passwords
- Scouring of Facebook, LinkedIn and other social media sources
- Emails from a misleading source with obscured or modified origin (ex: Amazon.com)

8

How are attacks initiated?

Email initiated cyber attacks can start in a number of ways:



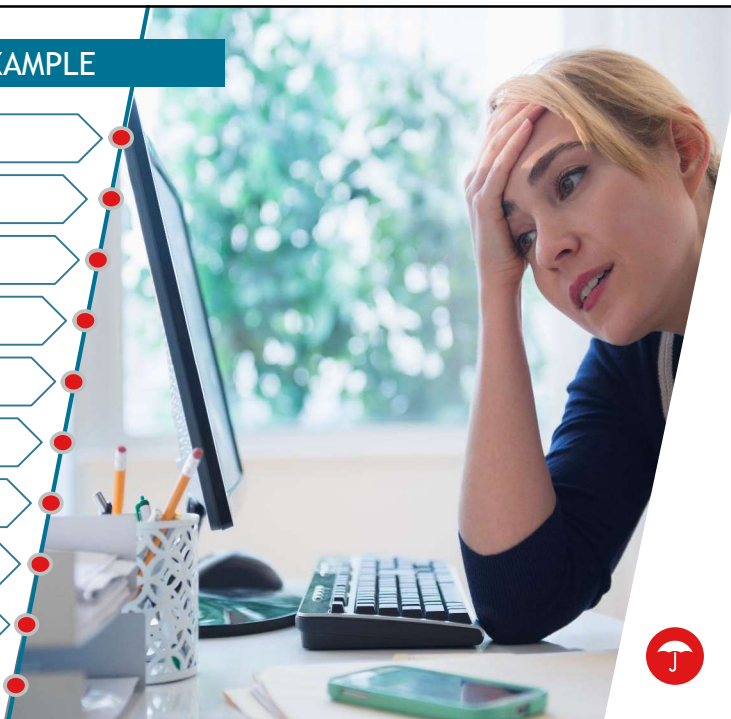
- Criminals alter settings for compromised account
- TAs monitor email traffic to understand organizational structure, speech nuances, etc. to inflict maximum damage
- Damage can come from accessing corporate intellectual property, databases, personnel files or customer and vendor information
- Hackers 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



9

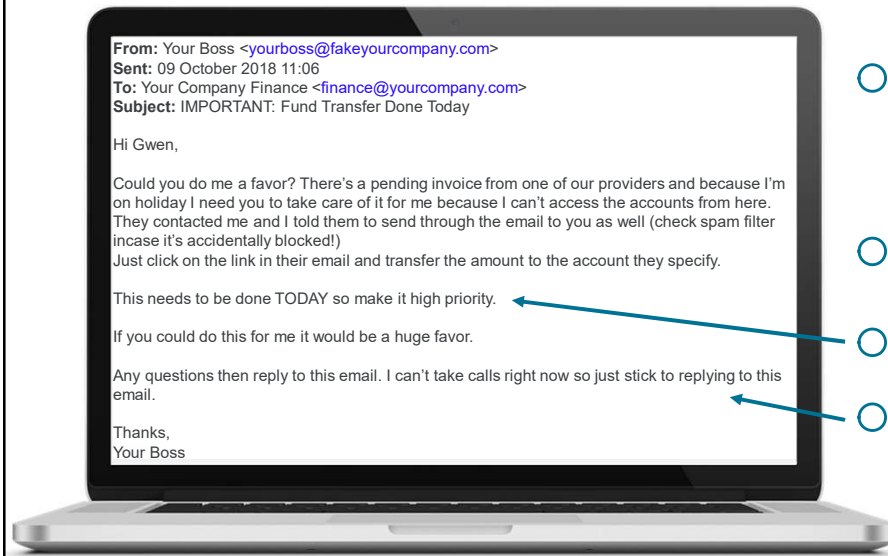
Email Compromise Attack Chain EXAMPLE

- TA obtains login credentials for email account
- TA logs onto account and monitors traffic
- TA modifies email auto-forwarding rules
- TA initiates emails internally and externally
- TA emails customer inquiring on payment of bill
- TA mentions banking information has changed
- Customer sends payment to fraudster's bank
- Authorized user asks customer about payment due
- Customer indicates the bill has been paid
- Authorized user realizes their account and possible corporate network are compromised



10

Email Compromise: Employee to Employee

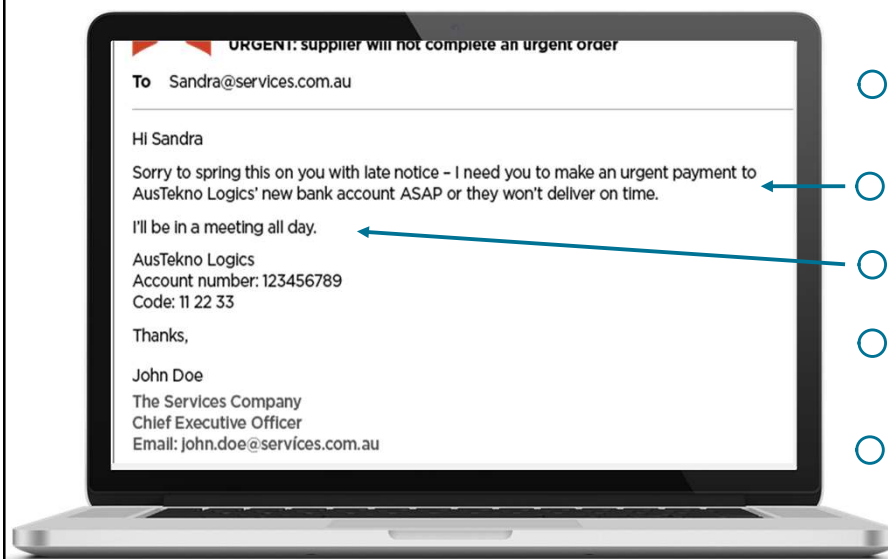


- TA targeting a subordinate—common tactic to pray on a person’s willingness to please a superior
- Separate email sent with malicious link
- Urgent request—common tactic
- Sender can’t be reached—common tactic



11

Email Compromise: Employee to Employee



- 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



12

E-mail compromise LOSS PREVENTION

- Require multi-factor authentication (MFA) for email & 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 & password
- Employ robust email filtering tools
- Block or alert new auto-forwarding rules



13

Top threats: Ransomware




14

Ransomware:







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

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



15

Ransomware (continues to intensify)

 <p>More TAs and evolving variants</p>	 <p>Attacker persistence</p>	 <p>Ransomware as a Service (RaaS)</p>
 <p>Evolving cryptocurrencies and valuation</p>	 <p>Ransom demand amounts increasing and groups threatening to release data</p>	 <p>Shared computer systems</p>

16

Ransomware LOSS PREVENTION

System security controls and maintenance



17

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 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




18

Top threats: Credential theft and failure to patch




19

Credential theft & failure to patch




TAs frequently target individuals who have IT administrator credentials




Gaining control of an administrator's credentials/login information is TA's main objective

Administrators can do things like configure and access:



- Active directory
- Email settings
- Servers, both on premises and cloud
- Anti-virus/EDR/firewalls/email filters
- Patches
- Backups, both on premises and cloud
- Web browser settings



20

Credential theft & failure to patch LOSS PREVENTION

- 1 Secure the credentials of those with administrator access/privileged access



- Separate account for IT work
- MFA should be required
- Disable “local admin” from computers
- Consider using a Privileged Access Management (PAM) tool

- 2 Track all corporate IT assets – you need to know what you have in order to protect it

- 3 Regularly update/patch corporate assets with expedited process for critical patches



- Most vulnerabilities had free patches available at the time the organization was attacked
- Microsoft’s “Patch Tuesday” routinely includes 100+ security patches each month



21


Important concepts



22

What is multi-factor authentication (MFA)?

MFA is a critical added layer of protection



MFA requires at least 2 of the following 3 factors

- 1 something you know
- 2 something you have
- 3 something you are


Most IT professionals consider MFA one of the **most important security controls** that can be deployed

MFA is sometimes confused with VPN. **VPN** encrypts communications; **MFA** is attempting to making sure the **RIGHT** person is accessing or using something

A username and password by itself would **NOT** be considered MFA

Two factor authentication is a form of MFA


Adaptive MFA and PAM are becoming more widely used



23

IP addresses & ports

There are roughly **65,000** ports




- 443 Secure web browsing
- 3389 Default RDP port
- 445 File & printer sharing


Particularly enticing for criminals intent on doing harm to organizations

Closing these ports can help reduce the potential attack surface of an organization

TAs utilize port scanning tools to search for ports that are open to internet and for unpatched vulnerabilities



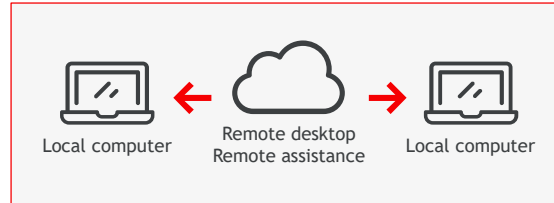
Organizations should consider scanning their network to see what ports are observable and open



24

What is Remote Desktop Protocol (RDP)?

RDP is a default tool included in Windows that **allows for a computer** (ex: laptop) **to connect to a local computer** (at work)



3389

RDP uses port **3389** to accomplish this connection

- Many smaller organizations use this default setup given the simplicity and no additional expense
- Unfortunately, it is a well-known port to all cyber criminals
- The BlueKeep vulnerability (CVE-2019-0708) that caused a panic in 2019 was an RDP exploit
- RDP has had numerous serious vulnerabilities over the years
- While security measures can help minimize risk, closing port 3389 is the best course of action



25

By-the-numbers



26

Cyber claims & incidents

Q3 2021 to Q4 2021 Coveware reported

↑130%

increase in ransomware payments. Additionally, Coveware reports that 84% of ransomware includes data exfiltration

2021 Verizon reported

61%

of breaches attributed to leveraged credentials

2020 Microsoft stated

99.9%

of compromised accounts did not use MFA

Many cybersecurity breaches involve human error – failure to patch, misconfiguration of security applications or clicking on malicious links



Sources: <https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021>; Verizon 2021 DBIR Report; <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>

27

Cyber claim themes



28

Cyber claim themes

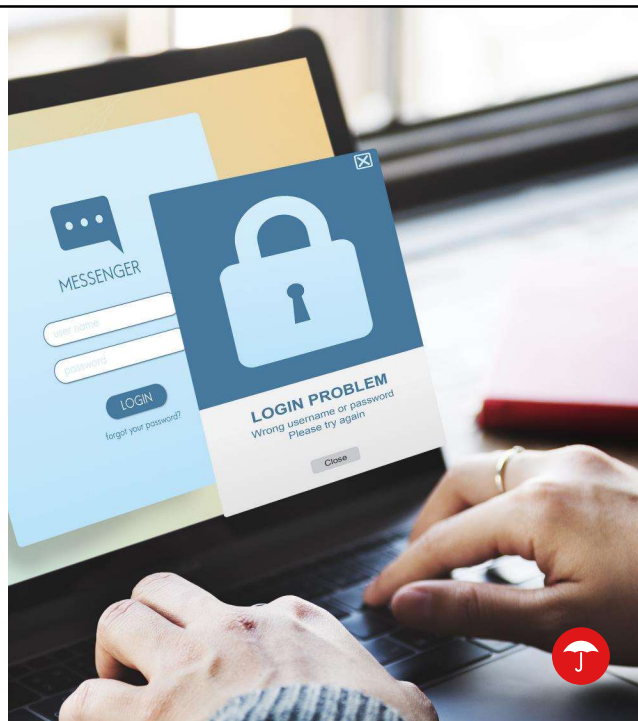
- Inadequate protection of administrator credentials (no MFA for remote or on premises, no separate administrator account)
- No MFA for remote connection to environment, either cloud or premises
- Improperly configured security tools
- RDP port 3389 & 445 open
- Organizations don't test validity of their backups



29

Cyber claim themes

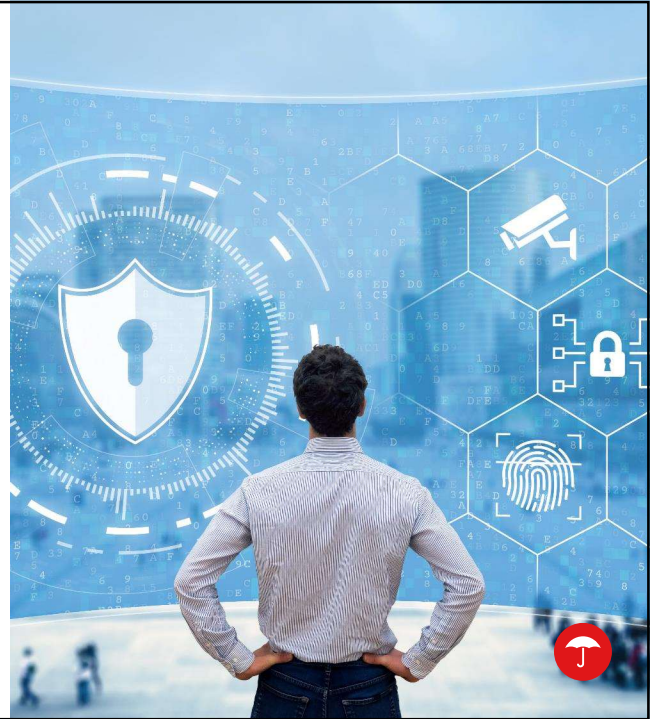
- Little or no visibility or tracking of corporate assets—EDR can help with this
- Insufficient endpoint protection or email filtering
- Insufficient onboarding and recurring training of employees
- Unqualified or understaffed IT departments
- Running End of Life (EOL) applications/hardware



30

Cyber claim themes

- No robust patch management procedures
- No vendor management or vendor review process
- Organizations not taking cyber security and integrity of their environment seriously
- No established or regularly practiced incident response plan



31

Cyber insurance



32

Four areas of coverage



LIABILITY	BUSINESS LOSS	BREACH RESPONSE	CYBER CRIME
<ul style="list-style-type: none"> • Privacy & security • Media • Regulatory 	<ul style="list-style-type: none"> • Business interruption • Dependent business interruption • System failure • Reputation harm 	<ul style="list-style-type: none"> • Privacy breach notification • Computer & legal experts • Public relations • Cyber extortion • Data restoration 	<ul style="list-style-type: none"> • Computer fraud • Funds transfer fraud • Social engineering fraud • Telecom fraud



33

Why buy cyber insurance?

- Breach coach can help quickly establish a plan of action
- Most carriers offer risk mitigation tools & information
- With Pay on Behalf language, insurance helps minimize the financial strain of having to potentially shell out significant amounts of money in a short amount of time
- Breach Coach helps guide insured & performs critical services
- Forensic review of network/environment can lead to improvements in overall security



34

Questions

