Preparing Your Leadership for a Ransomware Attack

National Association of State Treasurers

Disclaimer

Chase, J.P. Morgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its affiliates and subsidiaries worldwide (collectively, "JPMC", "We", "Our" or "Us", as the context may require).

We prepared these materials for discussion purposes only and for your sole and exclusive benefit. This information is confidential and proprietary to our firm and may only be used by you to evaluate the products and services described here. You may not copy, publish, disclose or use this information for any other purpose unless you receive our express authorization.

These materials do not represent an offer or commitment to provide any product or service. In preparing the information, we have relied upon, without independently verifying, the accuracy and completeness of publicly available information or information that you have provided to us. Our opinions, analyses and estimates included here reflect prevailing conditions and our views as of this date. These factors could change, and you should consider this information to be indicative, preliminary and for illustrative purposes only. This Information is provided as general market and/or economic commentary. It in no way constitutes research and should not be treated as such.

The information is not advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting, or similar advisors before entering into any agreement for our products or services. In no event shall JPMC or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon or for any inaccuracies or errors in, or omissions from, the information in this material. We are not acting as your agent, fiduciary or advisor, including, without limitation, as a Municipal Advisor under the Securities and Exchange Act of 1934.

The information does not include all applicable terms or issues and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, eligibility for particular products and services is subject to satisfaction of applicable legal, tax, risk, credit and other due diligence, JPMC's "know your customer," anti-money laundering, anti-terrorism and other policies and procedures.

Products and services may be provided by Commercial Banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by Commercial Banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any Commercial Banking affiliate and are not insured by the Federal Deposit Insurance Corporation.

Changes to Interbank Offered Rates (IBORs) and other benchmark rates: Certain interest rate benchmarks are, or may in the future become, subject to ongoing international, national and other regulatory guidance, reform and proposals for reform. For more information, please consult: https://www.jpmorgan.com/global/disclosures/interbank_offered_rates.

JPMorgan Chase Bank, N.A. Member FDIC.

Agenda

Exercise Flow (all times ET)

Time	Duration (in mins)	Event
3:00 - 3:15 pm	15	Threat Landscape Update
3:15 - 3:20 pm	5	Tabletop Exercise Overview & Guidelines
3:20 - 3:30 pm	10	Inject 1: Scenario Brief & Polling / Discussion
3:30 - 3:40 pm	10	Inject 2: Scenario Brief & Polling / Discussion
3:40 - 3:50 pm	10	Inject 3: Scenario Brief & Polling / Discussion
3:50 - 4:00 pm	10	Lessons Learned and Q&A

Threat Landscape Update

Threat Landscape Update

Bad actors continuously seek to leverage emerging technology and vulnerabilities to carry out malicious activity…

Kronos Ransomware attack could impact employee paychecks and timesheets for weeks

By Jennifer Korm

Updated 8.07 AM ET, Fri December 17, 2021

LILY HAY NEWMAN SECURITY 12.08.2021

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russian-led campaign was wake-up call to the industry, but there's no one solution to the threat.

Attackers Exploit Log4j Flaws in Hands-on Keyboard Attacks to Drop Reserve Shells

Microsoft says vulnerabilities present a "real and present" danger, citing high volume of scanning and attack activity targeting the widely used Apache logging framework

The Money Times

Banking Fraud Using Communication Devices Rose By More Than 65% Post COVID

Exercise Overview

- This tabletop exercise consists of realistic scenarios based on current threats and historic examples of actual cyber crises – it is not based upon any intelligence indicating a specific threat to your organization
- This type of incident has resulted in legal & regulatory action, media attention, and financial loss
- The exercise is designed to emphasize and examine roles & responsibilities as well as key decisions that organizations must make during a cyber event

Key Objectives

- ☑ **Highlight and develop the skills to lead and work through a cyber incident**
- ☑ **Understand all relevant stakeholders required to respond to a significant breach**
- ☑ **Learn how to conduct an exercise that could be used to test your agency's breach preparedness**
- ☑ **Take away ideas for how your company could improve its incident response plan**

State of the World

- You work for the State Treasurer's Office in the fictional state of Winnemac as part of the executive leadership team. Your office is responsible for a wide range of duties including receiving and depositing state funds, managing investments, and tracking budget surpluses/deficits.

- 1 hour virtual, discussion-based exercise

- The scenario will be presented across three days

- New facts will be provided each day as the investigation unfolds

- At the end of each day/inject, participants will answer polling questions

- Polling responses will then be discussed amongst the larger group

START OF EXERCISE *("STARTEX")*

Day 1

Detection and Initial Impacts

Day #1: Tuesday, October 11, 2022, 10:00am ET

- Employees at the Winnemac State Treasurer's Office report user account lockouts and logon failures to the IT Department. Additional issues include increased network latency (e.g., internal web pages and applications are taking a long time to load properly)
- The IT Department receives alerts about unauthorized admin security settings
- Some analysts can see alerts, but cannot take actions as they are also locked out
- The root cause of the issue is being investigated

Polling Questions

1 | Who would you inform first once made aware of the ongoing issue?

A Law Enforcement

B Managed Security Services Provider (MSSP), if applicable

C State Leaders (i.e., Treasurer, Governor)

D Crisis Management / Incident Response team

E All of the above

Polling Questions

2 | At this point in time, are you coordinating with communications personnel regarding internal and external messaging?

A Yes

B No

C I'm not sure

Day 2

Response and Validation

Day #2: Wednesday, October 12, 2022, 8:00am ET

- Employees trying to login begin receiving a pop-up message from the Anti-Justice League (AJL). The pop-up is an extortion demand for $10MM USD in Bitcoin. Further investigation reveals AJL discovered privileged Active Directory credentials on an unrestricted file share and proceeded to leverage them to obtain code execution on the Office of the Treasurer's domain. This access was then used to deploy malware throughout the network.

HACKED! ✖

Hello State of Winnemac,

Surprise! We've encrypted your critical payment files and systems. You have 72 hours to pay us $10MM USD in Bitcoin. If you pay, we will send you the decryption key to get your files back. If you don't meet our timeline, your data will be lost forever. We are attaching a small sample of the data to prove we have it. Follow the link for **payment instructions**.

Regards,
Anti-Justice League

Polling Questions

3 | How would you advise your State Treasurer to respond to the situation?

A Pay the extortion demand to return to normal business operations ASAP

B Contact law enforcement for assistance

C Investigate the scope of the compromise and isolate the affected parts of the network

D Contact a third-party incident response or cybersecurity insurance provider

E Contact the adversary to potentially negotiate the extortion demand (either directly or through an intermediary)

F A combination of C-E simultaneously

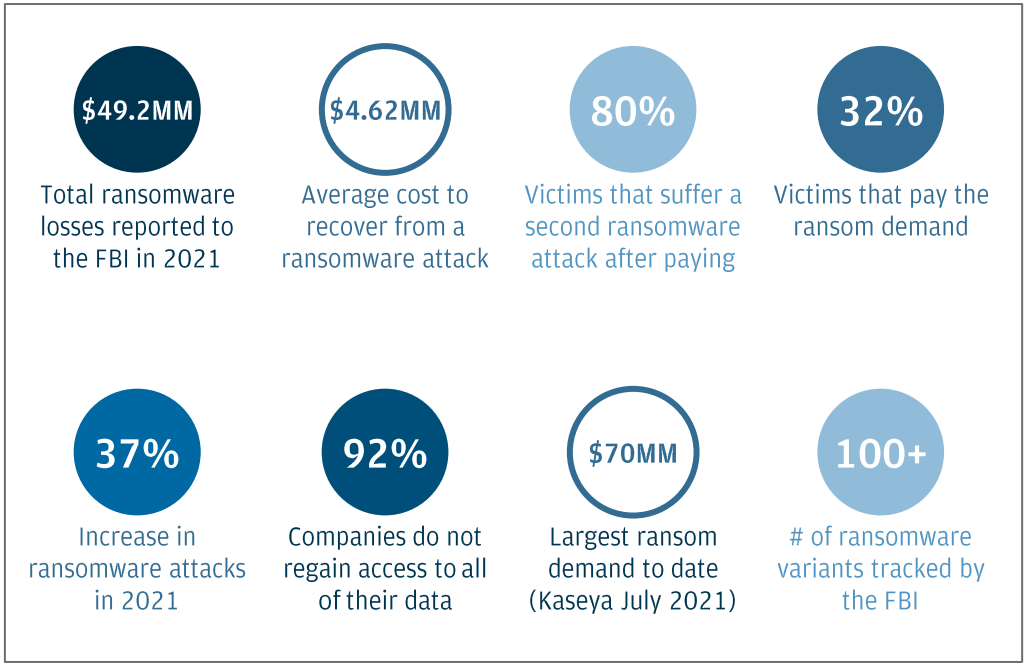
Ransomware poses an increased threat to organizations

Attacks are increasing in scale and frequency

- Ransomware operations function like a business
- 'Big Game Hunting' prioritizes high-value targets
- Ransomware-as-a-Service broadens pool of attackers
- 3,729 ransomware incidents were reported in 2021, up 37% from 2020
- In 2021, ransomware demands appear to be bigger and targeting more critical infrastructure, particularly hospitals and healthcare

Paying may seem like the most attractive option

- Double and Triple extortion and other techniques increase pressure on victims to pay
- Cyber insurance has been widely adopted
- Incident response takes significant time and money
- Attackers make negotiation communications and payment simple



Day 3

Incident Wind Down and Communications

Day #3: Thursday, October 12, 2022, 8:00am ET

- News of the ransomware attack have reached mainstream media channels. Outlets are asking the State Treasurer's Office for comment. The Governor of Winnemac is asking leadership for a status update and way ahead.

Polling Questions

4 | How are you handling external messaging?

A Hold off on making any public statement

B Release a statement that there has been a technical issue resulting in business impact and it is under investigation

C Make a generic statement that there has been a cyber attack but don't go into any details

D Confirm that Winnemac has fallen victim to a ransomware attack and personnel are able to access the network

E Hold a press conference and reveal the full impact to Winnemac

F None of the above

Polling Questions

5 | Do personnel know how to handle media requests in the event of a cyber incident?

A Yes

B No

C I'm not sure

END OF EXERCISE *("ENDEX")*

Thank you for your participation!

Tips to Better Protect Your Organization

1. **Conduct an independent assessment** – Engage an experienced engineering firm that understands the technical risks and complexities of enterprise architecture to do a complete technical independent assessment of your firm's infrastructure. Make sure to engage a company that has more technical expertise than a general consulting firm. You should know where your vulnerabilities are always
2. **Engage government and law enforcement** – Ensure you have a clear engagement model with the government including law enforcement. Who are you going to call? Which agency and under what circumstances? Have the relationship established up front and the engagement documented in a run book
3. **Join an industry forum** – Join an applicable industry-based information sharing forum ("ISAC") to share and receive important threat information
4. **Simulate an internal attack** – Create a Red Team and have them attack your systems using the same techniques the bad guys do. Not once a year, all the time. Also consider establishing a program to harvest credentials and account numbers that might be in the underground related to your bank–to detect compromises you may not otherwise be aware of
5. **Deploy mandatory employee training and testing** – Malicious email is the #1-way bad guys get into organizations. Establish a baseline training program for all employees that is mandatory and focuses on the specific actions employees need to take to protect the firm. Once you have trained your employees, actively test them. For example, start sending your employees targeted phishing and require those who click in the phishing emails to take additional training
6. **Know your third-party vendors** – Understand your third-party environment and upgrade your contract provisions and ensure they are following the same standards you are striving for in your own environments
7. **Exercises and drills** – Run simulations and drills to assess your capability. Use a combination of tabletop scenario exercises and live inject of events into your Security Operations Centers to see how it responds. Learn lessons and repeat. Include colleagues from the business in addition to technologists in the tabletop exercises
8. **Know how money leaves the organization** – Look at all of the ways money leaves your institution. Figure out what controls and thresholds you can put in to protect money movement assuming bad guys get around your other controls. Examples: wire limits, country destinations, new beneficiaries
9. **Implement controls for maximum effect –** Consider using JPMC resources such as Positive Pay, Reverse Positive Pay, ACH Debit Blocking, and ACH Transaction Review to provide early warning of potentially fraudulent activity, allowing for faster intervention and increased likelihood of stopping transactions and recovering funds
10. **Protect your computers** – Consider physical or logical network segmentation for funds transfer related computers; employ the concept of 'least privilege" to limit the use of administrator privileges; and consider limiting the processes and services that can be run on funds transfer related computers (e.g., no email or Internet browser applications)