BANK OF AMERICA

FACT SHEET

# Preparing and Responding to a cyber incident

## Tips for keeping your company's operations coordinated before and after a disruption.

Cyber crime is a reality for businesses of every size and in every industry. As work processes evolve and become increasingly digitized, criminals are leveraging a variety of methods to target weaknesses in companies and their partner organizations. An effective response to a cyber breach may be the difference between an incident that creates a minor disruption and one that cripples a business.

While each cyber event creates unique challenges, businesses can institute processes around response, communication and recovery that can help contain the extent of data loss and system infection while helping protect the organization from follow-up incidents. Here are key elements that can be adapted to your company's distinctive response plan:

## 1 Preparation

**Consider** what types of cyber incidents are most likely to impact your business, and tailor response plans to address them.

**Identify and prioritize** your most valuable company data and create protocols for protecting or recovering it following a cyber event.

**Gain** buy-in from key decision-makers, especially those whose response during an event will be critical to recovery.

**Create** effective chains of command protocols and have decision-makers regularly review recovery scenarios.

**Secure** the services of preferred legal and recovery experts prior to any event and establish how you'll contact them if normal communications are interrupted.

**Establish** strong communication protocols outside of normal channels. Make sure that all decision-makers have provided multiple ways to contact them, including personal phone numbers and email accounts.

**Make sure** the cyber response plan is available to all decision-makers in formats that can be accessed even when primary company networks are compromised.

### Cyber Security by the Numbers

44%

Percentage of businesses with established plans for preventing and responding to cyber security incidents.[1]

$1 trillion

Global financial losses related to cyber events in 2020.[2]

1st

Rank of phishing among actions that lead to cyber breaches in 2020.[3]

[1] McAfee, "The Hidden Costs of Cyber Crime," December 2020.

[2] Ibid.

[3] Verizon, "Data Breach Investigations Report," 2020.

## 2 Detection and assessment

**Gather** all information about when and where the incident was first reported.

**Determine** the type of incident: e.g. ransomware encryption, data exfiltration, malware infection or release of proprietary information.

**Scan** all company networks to determine the extent of the intrusion or compromise.

**Notify** all decision-makers on the incident response team, even if the nature of the incident has yet to be determined.

**Begin** a log of the response effort and record any information about the nature of the incident to facilitate forensics and recovery.

## 3 Response and threat eradication

**Disconnect** all affected devices and network segments from company systems and the internet.

**Determine** if any business-critical data has been compromised, stolen or released.

**Eradicate** any files that are not mission-critical or can be restored through backups.

**Perform** updates or patches to company software and network security components to collect more information about the incident and prevent criminals from exploiting vulnerabilities a second time.

**Coordinate** the response team around internal and external communications.

**Consult** with legal experts concerning possible compliance implications, engagement with law enforcement and public accountability.

**Notify** relevant partner organizations or customers with factual statements that provide only details available at that moment, with assurance that more information is forthcoming.

**Prepare** questions for your IT security team, and be prepared to resolve issues that are not covered in the existing cyber response plan.

Cyber Security by the Numbers

$3.86 million

Global average cost of a data breach in 2020.[4]

[4] IBM Security, "Cost of a Data Breach Report," 2020.

$3.58 million

Average cost savings of fully deployed security automation vs. no security automation.[5]

[5] Ibid.

81%

Percentage of organizations that rated cyber incident response as "very important" in 2020.[6]

[6] Ponemon Institute, "Second Annual Study on the Economics of Security Operations Centers: What is the True Cost for Effective Results?" January 2021.

## 4 Recovery

**Instruct** all affected personnel to reset passwords and system access controls, preferably while utilizing multi-factor authentication or other similar authentication methods.

**Conduct** a system-wide scan of the company, led by either a designated recovery team or outside experts.

**Restore** all systems to their pre-incident status via backups once all evidence of the intrusion has been eradicated.

**Continue** to collect any forensic evidence of the incident that can inform a follow-up report and contribute to remediation.

**Update** all affected personnel when a report on the event is complete and incorporate relevant findings from it into the existing response plan and training procedures.

**Maintain** communication with partner organizations, customers or the public and inform them of remedial steps the company has taken to defend against future incidents.

**Incorporate** revised best practices around security, network access and cyber awareness into company culture and encourage all employees to remain alert to potential threats.

## Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe that work 24/7 to keep data and information safe.

*For more information, go to www.bankofamerica.com/privacy/overview.go.*

### IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided “as is,” with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

“Bank of America Merrill Lynch” is the marketing name for the global banking and global markets businesses of Bank of America Corporation, including Bank of America, N.A., Member FDIC.