

Be cyber secure: respond to cyber incidents



Cybercrime is a reality for businesses of every size and in every industry. As work processes evolve and become increasingly digitized, criminals leverage a variety of methods to target weaknesses in companies and their partner organizations. An effective response to a cyber breach may make 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:



Preparation

Consider what types of cyber incidents could most likely 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 they can access even if primary company networks become compromised.



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.



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.



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.



To learn more

The Global Information Security (GIS) team at Bank of America 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.

Visit www.bankofamerica.com/privacy/overview.go to learn how to help protect yourself and your business.

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" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value
-----------------------------	--------------------------------	-----------------------

© 2024 Bank of America Corporation. All rights reserved. 6967146