Be cyber secure: creating a cyber response plan

Businesses continue to be a focus for cyber criminals and those businesses that haven't put a proper cybersecurity strategy in place are most at risk. Through good planning and smart response processes, you can mitigate vulnerabilities and limit threats to your network.

Develop strong internal tools and processes

Create an incident response team

Assign participants clear roles and responsibilities by answering these questions: Who has the authority to make decisions? Who will track the event and communicate beginning to end?

Create a communications plan and workflow. Determine how team members will communicate, which channels are preferred and who will report to internal and external stakeholders when concerns arise.

Establish an information-gathering procedure to understand how incident details will be compiled, summarized and shared with your executives, teams and partners.

Gather contact information for all vendors and third-party suppliers.

Design playbooks to address cyber events

Build a step-by-step cyber response playbook that explains what to do when confronted with different types of cybersecurity events.

Conduct security testing of your apps, devices and IT infrastructure on a regular basis to identify vulnerabilities before they can be exploited.

Schedule time for teams to run tabletop exercises to validate playbook effectiveness.

Adopt a threat management model for addressing cyber events, should they arise.

Know where to turn to for help

Determine the person or team responsible for cybersecurity within each of your company's functional areas and include their names on a list of internal and external points of contact for distribution to your staff.

Include internal off-hours contact numbers, noting that many system breaches and network compromises are attempted after normal working hours, on weekends or on holidays.

Establish relationships with your legal, banking and cyber forensics teams before a cyber event occurs and understand who can quarantine or shut down systems, websites or services on short notice.

Identify the individuals and specialists you can draw on if you need immediate expertise, beyond the scope of your team, to assist your staff when unexpected cyber events arise.

Establish a communication strategy

Understand how you will share cyber incident information with each type of stakeholder: external partners, investors and the general public.

Use time-saving templates that standardize threat reports and updates, and highlight key incident details.

Protect your privacy and guard against leaks by creating secure communications channels.

Define threat severity levels and the circumstances in which you should further escalate concerns to additional stakeholders.

Identify sources of concern

Thoroughly investigate the root cause of any cyber incidents and share the results with your recovery teams.

Review past incidents periodically to verify that all lessons from the event have been incorporated into established risk mitigation plans.

Assess organizational performance during these incidents and decide where to give threat responders more autonomy to help boost response times.

Review your incident response plans quarterly, revisiting your strategies to find areas for improvement.

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 who work 24/7 to keep data and information safe.

Visit www.business.bofa.com/managingfraudrisk to learn how to help protect yourself and those closest to you.

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" 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 are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value