BANK OF AMERICA

FACT SHEET

Creating a Cyber Response Plan

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

Here are three things you can do now that could help reduce your company's cyber crime risk.

Inside

1 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 run point on incidents? Who will track the incident 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 cyber security incidents.

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 efficacy.

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

Cyber Security by the Numbers

$10.5 trillion

Estimated cost of cyber crime by 2025.

Cybersecurity Ventures Cybercrime Report.

62%

Percentage of incidents that involve non-malicous insiders.

Ponemon Institute, 2020 Cost of Insider Threats Global Report, January 2020.

Know where to turn for help

Determine the person or team responsible for cyber security 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 incident have been incorporated into established risk mitigation plans.

Assess organizational performance during these incidents to decide where threat responders can be given more autonomy to help boost response times.

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

Cyber Security by the Numbers

$3.86 million

Average total cost of a data breach.

IBM, Cost of a Data Breach Report, 2020.

119,000

Number of new threats released by cyber criminals each minute.

Infosecurity Magazine, 119,000 Threats Per Minute Detected in 2020, 2021.

43%

Percentage of all cyber strikes that are aimed at small businesses.

Verizon, Data Breach Report, 2019.

2 Be aware of the most current cyber threats

It is vital to be aware of the most common forms of cyber crime so you can prepare your defenses.

Malware
Malicious software designed to compromise or damage electronic devices.

Ransomware
Software designed to encrypt a computer system or systems until a ransom payment is made.

Identity theft
Stealing private information to assume another's identity.

Hacking
Unauthorized access to a digital device, computer system or network to obtain information, disrupt operations or promote malicious activity.

Phishing
The use of email from seemingly legitimate sources to elicit users to expose personal information to cyber criminals.

Social engineering
When cyber criminals pretend to be trusted individuals in order to trick users into giving out sensitive information.

Business email compromise (BEC)
When cyber criminals use business email to obtain sensitive information or perform fraudulent financial transactions.

Cyber Security by the Numbers

>2000

Number of complaints filed with the FBI on average per day.

FBI, IC3 Report, 2020.

900

Average number of cyber crime complaints received by the FBI each day.

(https://pdf.ic3.gov/2018_IC3Report.pdf)

280 days

Average time to identify and contain a data breach.

IBM, Cost of a Data Breach Report, 2020.

3 Promote positive cyber habits

Help employees understand that good cyber security begins with them, so they should speak up and say something if they spot suspicious activity.

Accept that it's OK to make mistakes as long as you don't repeat them. Share incident-related insights so that others can learn from them.

Review possible areas of risk exposure across your networks, systems and applications regularly, and consider how to minimize these risks.

Access current training programs regularly to identify opportunities for improvement.

Manage sensitive information, networks and communications carefully, and limit users' access to only those features or files that they need to perform a specific job.

Back up files and information on a daily or weekly basis, and store these backups in a secure location.

Conduct periodic drills that reinforce the procedures set out in your cyber recovery plan.

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

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