CYBERSECURITY

Why Cybersecurity Should be Top Priority for Your Financial Institutions

OnCourse Learning

Cybersecurity

Why Cybersecurity Should be Top Priority for Your Financial Institutions

Cybersecurity has become a growing concern as a number of large U.S. businesses have been victimized by major cyberattacks in recent years. Target, The Home Depot, Anthem Health Insurance and Sony Pictures are just some of the large corporations that have suffered high-profile attacks.

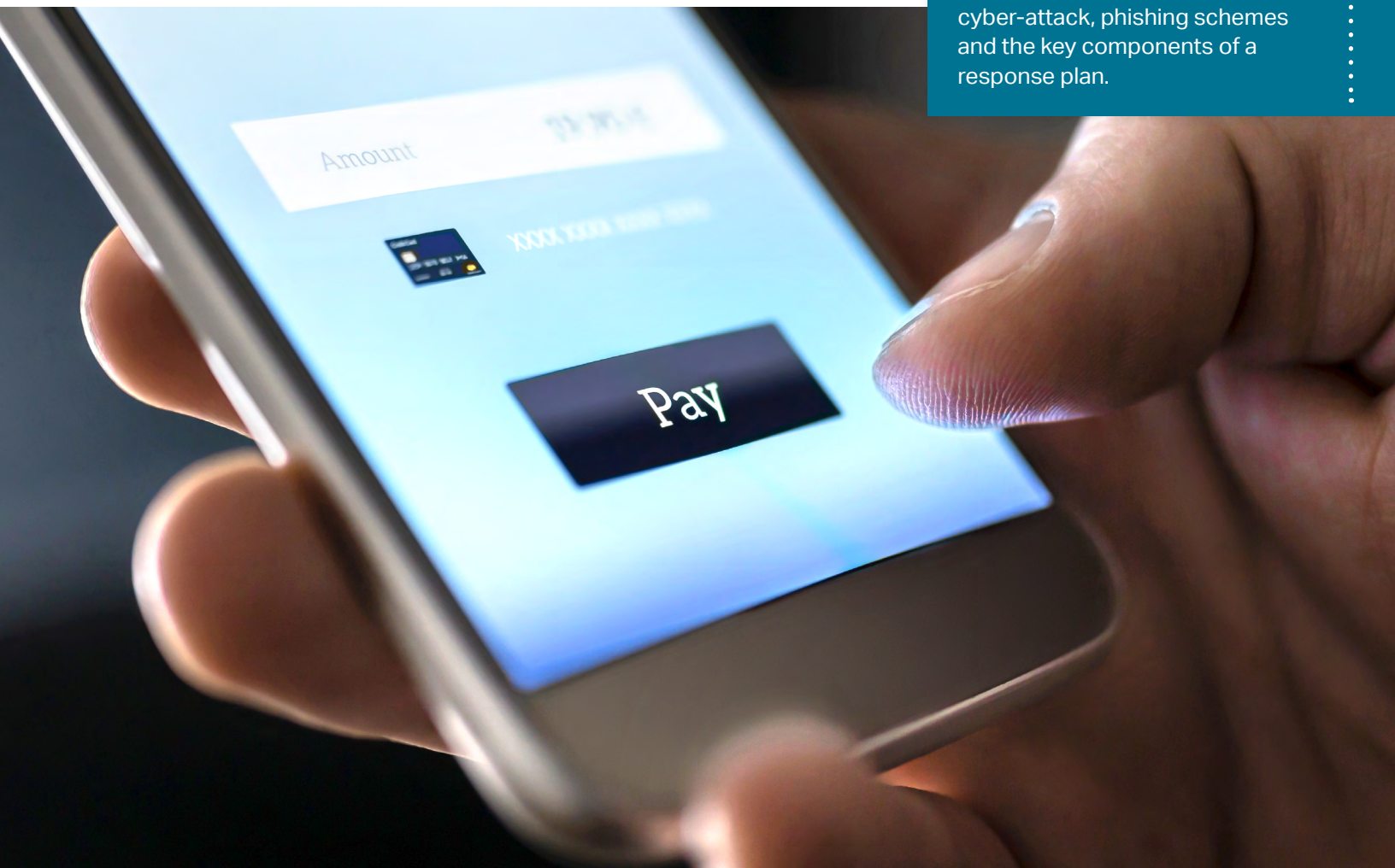
Unfortunately, banks are not immune to cyberattacks, as a computer breach at JPMorgan Chase a few years ago made clear. In this attack, the checking and savings account information of approximately 83 million households and small businesses was compromised. According to authorities, the hackers tried unsuccessfully to get into at least a dozen other financial institutions.

In this type of environment, it is critical that banks make cybersecurity a top priority.

TABLE OF CONTENTS

What to Expect

This ebook outlines the importance of cybersecurity. You'll learn about the cost of a cyber-attack, phishing schemes and the key components of a response plan.



Costs & Prevention of a **Cyberattack**

Banks can incur both hard and soft costs in the event of a cyberattack.

"First, banks must inform all affected customers whenever their personal identification or account information has been breached," says Senior Vice President and Deputy Chief Security Officer at Bank of the West. "Then they may have to pay for identity theft monitoring services of those customers, as well as for outside legal and forensics experts to come in and help after the attack. Banks might also face lawsuits from customers whose data was compromised."

Costs such as these are measurable, but the damage caused from weeks or months of bad publicity could be incalculable in terms of lost customers and reputational harm to the company's brand. In a worst-case scenario, the resulting costs potentially could be a fatal blow to a small or mid-sized bank that's unprepared to deal with the fallout from a cyberattack.

Cyberattacks
BEST PRACTICES

Because of the immense damage that can be caused by a cyberattack, cybersecurity experts[1] recommend that banks need to take proactive steps to improve cybersecurity.

The Federal Financial Institutions Examination Council has published a **list of steps >>** financial institutions should implement to help guard against a cyberattack.

- **Conduct** ongoing information security risk assessments
- **Perform** security monitoring, prevention and risk mitigation
- **Protect** against unauthorized access
- **Implement and test** controls around critical systems regularly
- **Manage** business continuity risk
- **Enhance** information security awareness and training programs
- **Participate** in industry information-sharing forums

$2.9 MILLION • $25/MINUTE

Every minute, $2.9 million is lost to cybercrime and top companies pay $25 per minute due to cybersecurity breaches.[2]

OnCourse Learning

Phishing **Schemes**

Banks often underestimate the human factor when planning their cyberattack defenses.

"Phishing and masquerading schemes are still among the main ways that hackers break into corporations and banks," states Senior Vice President and Deputy Chief Security Officer at Bank of the West. Masquerading scams - where cybercriminals send an email to employees that looks like it came from a high-level executive at a company, asking them to make some kind of electronic payment have added up to $3.1 billion in business costs over the past three years.

Therefore, it is critical banks train and educate all employees about what they should do if they receive a phishing or masquerading email. It's recommended to make sure employees know what to do if they mistakenly click on a link in one of these emails. Test your employees from time to time to see if they are following the cybersecurity procedures you've put in place.

To ensure appropriate cybersecurity measures are being taken, some banks consider hiring an outside company that specializes in cybersecurity training for employees. Specialized training can provide management with valuable insight into what kinds of cyberthreats are currently impacting financial institutions and the latest trends in cybersecurity. But it's also important for leaders to be actively involved in the training, since they tend to be them most familiar with internal processes.

...make sure employees know what to do if they **mistakenly click on a link** in one of these emails.

Response **Plan**

Even the best cyberattack defenses aren't foolproof. Many experts agree that if cybercriminals are determined to hack into a business or a bank, they may eventually succeed - even when strong security measures are taken. That's why it's critical to have a cyberattack incident response plan.

Cybersecurity experts recommend creating a Response Plan[1] prior to an attack. When establishing a response plan, it's important to identify threats and common attacks as well as practice scenarios.

Once an incident response plan is in place, test it periodically. By running tests based on simulations of different types of cyberattacks, leaders can ensure the response plan is working as expected.

With growing threats from terrorist groups, hackers and international criminal organization, the number of cyberattacks likely will only increase. Therefore, banks and other financial institutions need to be proactive and forward thinking to protect themselves and their customers. By investing in the latest cybersecurity measures and providing appropriate training for employees, banks can help minimize risks and reduce the likelihood of a costly breach and lasting damage to their reputation.

An incident response plan can help bank executives answer several key questions in the event of an attack.

RESTORE

How is your critical data being backed up and how will it be restored after an attack?

COMMUNICATE

Who is going to be your spokesperson with the media and how will you alert and communicate with your customers?

ESTABLISH

Do you have contracts in place with third-party service providers such as legal and forensics experts, who you may need to bring in after an attack?

References

1. 7 Steps to Building an Incident Response Playbook
   https://sbscyber.com/resources/7-steps-to-building-an-incident-response-playbook

2. Evil Internet Minute 2019 report from RiskIQ
   www.riskiq.com/infographic/evil-internet-minute-2019/

Ready *to*

MAKE CYBERSECURITY TOP PRIORITY?

OnCourse Learning provides a comprehensive solution for your compliance training and personal development needs.

Learn more at OnCourseLearning.com

OnCourse Learning is a member of the Adtalem Global Education Financial Services Workforce Solutions family which includes: the Association of Certified Anti-Money Laundering Specialists (ACAMS), its CAMS certification is one of the most widely recognized anti-money laundering certifications among compliance professionals worldwide; Becker Professional Education, which offers programs in CPA Exam Review and continuing professional education courses; and EduPristine, one of India's leading training providers in accounting, finance and digital marketing.

OnCourse Learning

CONTACT US

Contact OnCourse Learning for more information.

(866) 806 - 9900

www.OnCourseLearning.com