Why cybersecurity should be a **top priority** for your financial institution

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 aren't immune to cyberattacks, as a computer breach at JPMorgan Chase two 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.

> **"The costs of a cyberattack can be crippling to a small or mid-sized bank,"**
>
> — David Pollino, senior vice president and deputy chief security officer for Bank of the West.

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

Costs of a cyberattack

"The costs of a cyberattack can be crippling to a small or mid-sized bank," said David Pollino, senior vice president and deputy chief security officer for San Francisco-based Bank of the West.

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," Pollino said. "Then they may have to pay for identity theft monitoring services for these 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.

Preventing cyberattacks

Because of the immense damage that can be caused by a cyberattack, Pollino said 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.

These cybersecurity best practices include:

- 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.

Pollino said 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," Pollino said. 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 — cost businesses $3.1 billion over the past three years, he said.

Therefore, it is critical banks train and educate all employees about what they should do if they receive a phishing or masquerading email. "Just as important, make sure employees

Cyberattacks cost the average U.S. firm $15.4 million a year, more than double the global average

Source: 2015 Cost of Cyber Crime Study by Ponemon Institute and Hewlitt Packard

know what to do if they mistakenly click on a link in one of these emails, and test your employees from time to time to see if they are following the cybersecurity procedures you've put in place," Pollino said.

To ensure appropriate cybersecurity measures are being taken, some banks consider hiring an outside company that specializes in cybersecurity training for employees.

"This will provide management with valuable insight into what kinds of cyberthreats are currently impacting financial institutions and the latest trends in cybersecurity," Pollino said. "But it's also important to be actively involved in the training yourself, since you're most familiar with your internal processes and how things work in your bank."

Incident response plan

Even the best cyberattack defenses aren't foolproof, however. 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.

"You can't wait until after a cyberattack occurs to plan your response," Pollino said. "Think through all the possible scenarios that could occur in the event of a cyberattack and then plan for how you'll respond to these events."

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

- How is your critical data being backed up and how will it be restored after an attack?
- Who is going to be your spokesperson with the media?
- How will you communicate with and alert your customers?
- 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?

Once an incident response plan is in place, Pollino recommends it be tested periodically. "Run tests based on simulations of different types of cyberattacks to make sure your plan is working like it should," he said.

With growing threats from hackers, international criminal organizations and terrorist groups, 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.