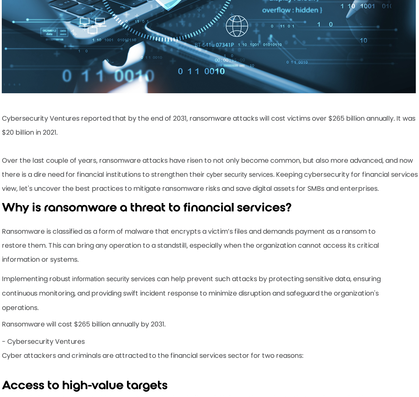
Blog

Cybersecurity for financial services: Best practices to mitigate ransomware risks

By *NETSOL Technologies*, on September 27, 2024

Explore the importance of cybersecurity for financial services in safeguarding your sensitive data. Learn best practices to mitigate evolving ransomware risks.



Cybersecurity Ventures reported that by the end of 2031, ransomware attacks will cost victims over $265 billion annually. It was $20 billion in 2021.

Over the last couple of years, ransomware attacks have risen to not only become common, but also more advanced, and now there is a dire need for financial institutions to strengthen their cyber security services. Keeping cybersecurity for financial services in view, let's uncover the best practices to mitigate ransomware risks and save digital assets for SMBs and enterprises.

Why is ransomware a threat to financial services?

Ransomware is classified as a form of malware that encrypts a victim's files and demands payment as a ransom to restore them. This can bring any operation to a standstill, especially when the organization cannot access its critical information or systems.

Implementing robust information security services can help prevent such attacks by protecting sensitive data, ensuring continuous monitoring, and providing swift incident response to minimize disruption and safeguard the organization's operations.

Ransomware will cost $265 billion annually by 2031.

- Cybersecurity Ventures

Cyber attackers and criminals are attracted to the financial services sector for two reasons:

Access to high-value targets

These criminals get access to highly sensitive and valuable financial information and data that can jeopardize the security and misuse of digital assets.

Motive to pay

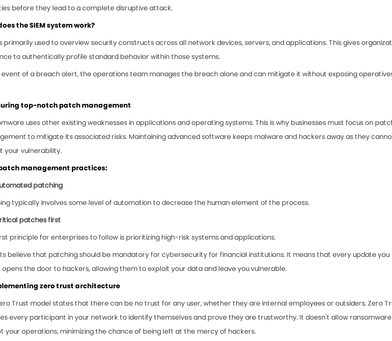
Financial firms often feel a greater need to pay the ransom quickly to resume business operations. The longer the downtime, the more loss they will suffer.

According to the former CEO of Cisco, John T. Chambers, "There are two types of companies: those who have been hacked, and those who don't know they've been hacked." This rings especially true for financial services, where a data breach can have devastating reputational and financial consequences.

There are two types of companies - those who have been hacked, and those who don't know they've been hacked. - John Chambers, former CEO, Cisco

Best practices to mitigate ransomware risks

As the ransomware threat escalates, financial institutions must adopt best practices to neutralize the threat and stay ahead of the curve.



1. Regularly backup the data

How can an organization limit the damage of a ransomware attack? Regular data backups are perhaps the most straightforward yet trustworthy measures available. Financial cybersecurity experts recommend offsite storage, preferably with encrypted backups. This allows for a highly security-focused organization that doesn't surrender to a demand for ransom.

How to implement effective backup strategies:

- Conduct regular backup verification to maintain quality.
- Implement air-gapped storage solutions to maintain copies of data that will be out of reach from any network connection.

2. Training employees and ensuring awareness

Mitigating inside threats is the most challenging aspect of cybersecurity. A successful attempt to extort a company with ransomware begins with a phishing email or a malicious link opened by an employee. Therefore, educating your employees on how to recognize phishing attacks and observing the best cyber hygiene practices is paramount to combatting revocation of access via ransomware.

Key training measures:

- Phishing simulations

Organize regular mock phishing intrusion drills for employees to help them stay alert. This will help them recognize the pattern of any potential unforeseen circumstances.

- Multi-factor authentication (MFA)

Minimize the risk of stolen usernames and passwords by adopting the habit of using multi-factor authentication wherever possible. MFA makes it harder for cybercriminals to crack the code and exploit your vulnerable data.

3. Using advanced threat detection systems

Advanced threat detection systems, such as Endpoint Detection and Response (EDR) or Security Information and Event Management (SIEM) systems, help to address and manage threats pertaining to cybersecurity for financial services more proactively and effectively. These allow monitoring of the network activities in an organization in real-time and capture suspicious activities before they lead to a complete disruptive attack.

How does the SIEM system work?

SIEM is primarily used to overview security constructs across all network devices, servers, and applications. This gives organizations a chance to authentically profile standard behavior within those systems.

In the event of a breach alert, the operations team manages the breach alone and can mitigate it without exposing operatives to risk.

4. Ensuring top-notch patch management

Ransomware uses other existing weaknesses in applications and operating systems. This is why businesses must focus on patch management to mitigate its associated risks. Maintaining advanced software keeps malware and hackers away as they cannot exploit your vulnerability.

Best patch management practices:

- Automated patching

Patching typically involves some level of automation to decrease the human element of the process.

- Critical patches first

The first principle for enterprises to follow is prioritizing high-risk systems and applications.

Experts believe that patching should be mandatory for cybersecurity for financial institutions. It means that every update you reject opens the door to hackers, allowing them to exploit your data and leave you vulnerable.

5. Implementing zero trust architecture

The Zero Trust model states that there can be no trust for any user, whether they are internal employees or outsiders. Zero Trust requires every participant in your network to identify themselves and prove they are trustworthy. It doesn't allow ransomware to disrupt your operations, minimizing the chance of being left at the mercy of hackers.

How to implement zero trust:

- Micro-segmentation

Isolate the workloads and restrict the accessibility of the core applications as well.

- Least privilege access

Implement permit control to allow employees only to access data points and systems relevant to their roles.

6. Managing incident response plan

If an attack is possible, you should always be prepared that it can happen at any time. An Incident Response (IR) Plan makes you fully prepared and aware of what to do in the case of a ransomware attack. Such a plan should contain guidelines regarding communication with customers, steps of recovery in case of dissatisfaction, legal issues, and more.

Elements of a strong IR plan:

- Communication channels

Identify stakeholders who should be contacted in case of an attack.

- Response team

Ensure you have a robust management team ready to be deployed and take care of the incident. They should be trained to manage such situations and neutralize the attack.

- Legal and compliance

For robust financial cybersecurity, make sure you are capable of managing the legalities by having strategies in place for dealing with ransomware attacks.

ThriveDX, an EdTech solutions brand, shared that despite the high rates of cyberattacks, enterprises still don't have an effective plan to secure their data. Over 77% of businesses worldwide have no IR plan in place.
Over 77% of businesses don't have an incident response plan. - ThriveDX

7. Implementation of cyber insurance

More and more financial services firms reported ransomware incidents, and as the threat increases, so does the demand for cyber insurance to manage costs. With effective financial services cybersecurity and insurance, businesses might be unable to prevent these attacks, but it significantly minimizes the potential loss and speeds up the data recovery process.

Key features of cyber insurance

The coverage includes ransom payments and the cost of data recovery requirements. It also benefits product liability, particularly in cases of customer information leaks.

Mitigating ransomware in the financial services sector

Financial services are especially vulnerable to cyber-attacks and ransomware, which have become one of the most dangerous and prevalent concerns in the sector. However, the risk can be massively averted by following the best cybersecurity practices for financial services and employing a systematic approach.

With constant monitoring, creating awareness among employees, and updating the security model, businesses can secure their digital assets against malicious attacks and viruses.

Not sure how to manage Zero Trust architecture and create an incident response plan? Contact NETSOL today to get more information on how we can help you secure your business against vulnerabilities, enhance your business operations, and secure digital premises.