Cybersecurity in Financial Services

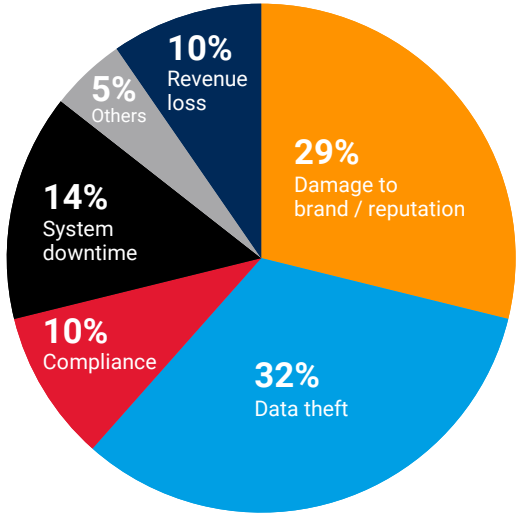
A view from APAC cyber leaders

The following insights are based on survey responses and discussions with cyber leaders in the financial services industry throughout the Asia-Pacific region.

Data theft top security risk

Financial institutions are one of the most appealing targets for cybercriminals. The average cost of a data breach in financial services is US $5.97 million — the second highest of any industry. Thus it is no surprise that cyber leaders in this survey believe the top business risk of a cyberattack is data theft.

What do you perceive as the key risk of a cyber attack to your business?

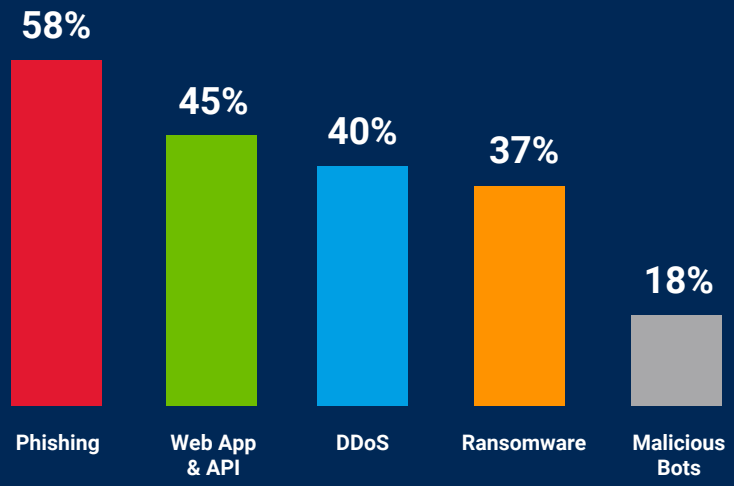


Recommendations:

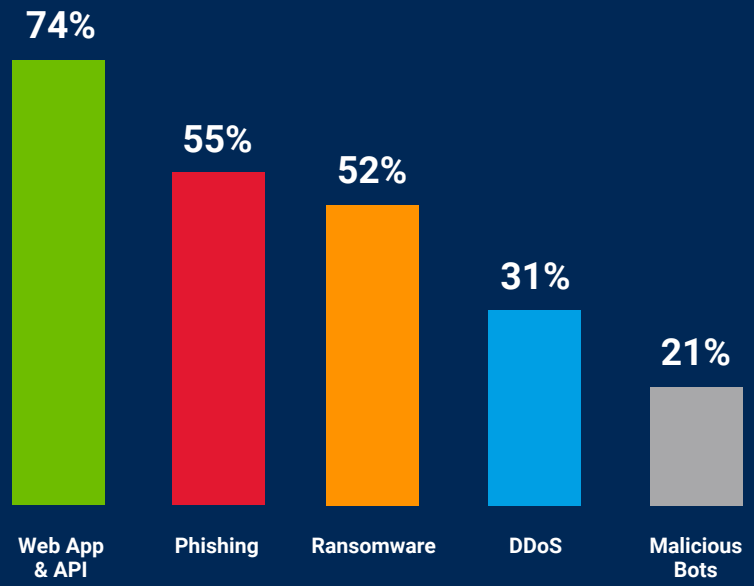
- Gain visibility into your critical applications and data, and their dependencies.
- Research common threat actors and their tactics, techniques, and procedures (TTPs).

Biggest cyberthreats in financial services

APAC cyber leaders in financial services reported a wide range of cyberattacks over the past 12 months.



Web app and API attacks are currently the top concern due to increasing frequency and sophistication of attacks.



Lack of visibility top API security issue

APIs are fueling innovation and rapid growth in the financial services industry. However, this also means that most financial services institutions face a rapidly expanding attack surface. Recent Akamai research showed a 36% year-over-year increase in web application and API attacks against financial services in APAC.

40%

of respondents said API discovery and lack of visibility into attack activity is the biggest API security issue they face.

Learn more:
Web Application and API Protection Capabilities:
A Checklist for Financial Institutions

Recommendations:

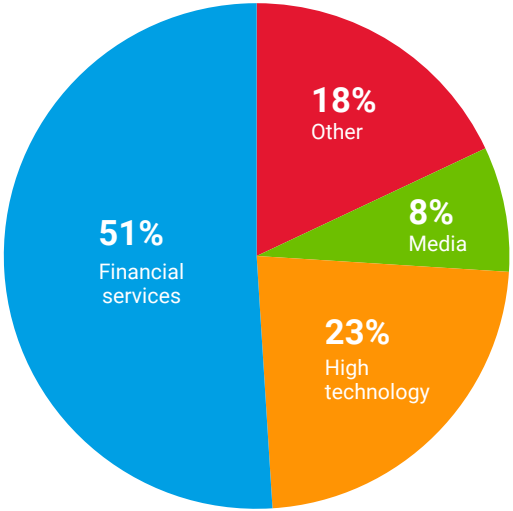
- Discover and catalog APIs
- Conduct API vulnerability testing and risk assessments
- Implement specialised API security tools
- Adopt a blanket set of API policies the can be used consistently across the organisation

Limited phishing visibility

Every week, more than 50,000 new phishing websites are created, yet 3 in 5 respondents have little to no visibility into this alarming surge. Most respondents try to address the risk through threat intelligence, detection, and takedown services for malicious websites.

Learn more:
The High Stakes of Innovation:
Attack Trends in Financial Services

Top targets of phishing attacks



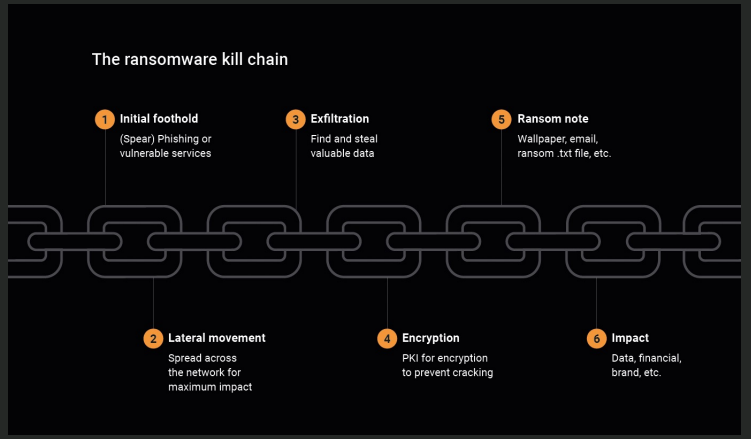
Source: The High Stakes of Innovation: Attack Trends in Financial Services

Recommendation:

- Consider updating phishing defences based on MFA bypass vulnerabilities and fake phishing websites.

The relentless pace of ransomware

Only 41% of cyber leaders in Asia-Pacific are confident of mitigating a ransomware attack. Legacy firewalls or perimeter-only defence can't stop ransomware from spreading across your network and locking down critical applications and infrastructure.



Learn more:
3 Ways Zero Trust Architecture Protects Your Financial Institution

Recommendations:

- Cut the ransomware killchain
- Stop lateral movement
- Implement a Zero Trust architecture

DDoS should remain on the radar

DDoS attacks targeting financial services increased 154% over the past year. The attacks can be large, distributed across the globe, and relatively easy to launch. They can also serve as a decoy, masking other more serious types of attacks.

Learn more:
DDoS: Here to Stay

Recommendation:

- DDoS preparedness should be based on an “always-on” mentality. Financial institutions should evaluate their attack surfaces in the context of the evolving threat landscape.

Malicious bots a major concern

Malicious bot requests surged by 69% year over year (as of 30 June 2023) and continue to be a growing threat to financial institutions and their customers. Malicious bots are often used for account takeover fraud and credential stuffing attacks.

Learn more:
The High Stakes of Innovation: Attack Trends in Financial Services

Recommendation:

- A superior bot mitigation solution will permit the activity of good bots while blocking malicious activity and botnet attacks. Even good bots need to be managed with techniques like slowing down good bots at times when your site has significant human traffic.

Need senior leadership buy-in to invest in security

Cyber leaders are under pressure to keep up with cyberthreats, but a range of organisational barriers stand in the way of increased investments in security.

33%

said a high risk tolerance is standing in the way of increased investment

57%

said senior leadership doesn't believe the risk justifies additional security investments

33%

lack sufficient resources to implement new security controls

Recommendations:

- Meet regularly with senior leaders and the board to share insights on cyberthreats.
- Quantify the budget and resources required to keep the business, employees, and customers safe from the growing security risk.

Recommendations

1. Update your incident response playbooks in preparation of increased velocity of attacks and increased volume of exploit attempts.

2. Understand your expanding attack surfaces and risk exposures to help you devise mitigation plans.

3. Review and implement risk models to determine if you have appropriate fraud and customer-based and fraud threats addressed.

4. Stay up to date on constantly evolving attack trends, and be prepared to adapt your cyber risk and security strategy to address them.

5. Meet regularly with senior leaders and the board to share insights on cyberthreats, and communicate what budget and resources are required.

Akamai for Financial Services

Protecting customer data and mitigating attacks for uninterrupted business

Akamai has successfully protected leading financial institutions around the globe from large-scale attacks, keeping their digital properties and applications up and running while safeguarding customer data.

Financial services institutions around the world trust Akamai

44
of the top
50 brokerages

10
of the top
10 banks

7
of the top 10
fintech companies

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog or follow Akamai Technologies on Twitter and LinkedIn.