Digital innovation?  □
Cyber secure?  □

Digital security: a Financial Services perspective

The better the question. The better the answer. The better the world works.
Contents

// Protecting your digital strategy in an evolving cyber environment 1
// What’s included in a comprehensive digital risk approach? 2
  // Asset risk identification 3
  // Legal and regulatory
  // Cloud management
// Process and technology controls 4
  // Application distribution 5
  // On-boarding customers quickly and securely
  // Third-party ecosystem management 6
  // Proactive monitoring
  // Service availability
// Incident response 7
  // Social and mobile management
  // Education and user awareness
// Let’s talk cybersecurity 8
As financial services institutions pursue digital strategies, their operations become part of an evolving cyber environment. In this connected ecosystem of entities, people and data, your organization is increasingly using web, mobile and social channels to transact with your customers and partners. This means the perimeter of your organization is disappearing. Mobile computing is blurring organizational boundaries, taking IT closer to the customer. We have opened up new avenues of cost saving, agility and speed to market.

To succeed in this environment, we believe institutions need six, equally important digital capabilities.

To **grow** through:
1. Increased revenue conversion (digital transactions)
2. Enhanced user experience

To **optimize** through:
3. A competitive digital strategy
4. Transforming the way people work

To **protect and comply** by:
5. Creating digital trust
6. Ensuring privacy

This paper focuses on an essential element required to protect and comply: implementing an effective and efficient cybersecurity strategy to protect and enable your digital investments.
What’s included in a comprehensive cybersecurity strategy to protect and enable your digital strategies?

Financial services providers need a comprehensive cybersecurity strategy that integrates with all their digital strategies.

Rather than adding on cybersecurity at the end of the digital transformation process, leading institutions are building their digital assets on the top of a holistic cybersecurity strategy. This ensures digital strategies are secured against digital risk from the outset and remain protected in a continually evolving cyber environment. The alternative — retrofitting cybersecurity — is expensive and often dangerously ineffective.

Managing cybersecurity correctly is as important to your customers, as it is to your shareholders. Customers are increasingly concerned about the security of their personal information and financial assets held by their financial services providers. As consumers become increasingly cyber savvy, they are also starting to view cybersecurity measures taken by institutions as an important criteria when choosing with whom to do business.

In fact, customers are so concerned about cybersecurity that a strong cybersecurity strategy can be an important marketing tool — enhancing their value proposition. Similarly, it can also be promoted to regulators, shareholders, business partners and suppliers, who are also increasingly focused on the cyber resilience of the financial services providers they engage with.

Cybersecurity strategy components

To protect your institution’s brand, intellectual property (IP) and customer data, while ensuring availability and a strong customer experience, your cybersecurity strategy should encompass:

- Asset risk identification
- Legal and regulatory
- Cloud management
- Process and technology controls
- Third-party ecosystem management
- Proactive monitoring
- Service availability
- Incident response
- Social and mobile management
- Education and user awareness
Asset risk identification

When institutions begin to plan their digital strategies, they often ignore digital asset risk. Digital asset risk is perceived as an IT issue — not as a core business risk. We consider digital risk to be just as important as market risk, brand risk and credit risk.

Assess asset risk upfront

- Identify the digital assets that are exposed by your digital strategy. This will include your: IP, people information, financial information, business information (strategy, performance, transactions), plus customer and third party data.
- Rank these assets in order of importance to your organization.
- Design risk mitigation into your digital strategy, aligned to the importance of these assets.

Legal and regulatory

Most Asia-Pacific jurisdictions have implemented privacy regulations strictly governing how customer data is collected, transmitted, manipulated and stored. Material fines and other regulatory imposts are now imposed on organizations failing to comply with these regulations.

At the same time, regulators are also increasingly focused on ensuring regulated entities have strong cybersecurity controls in place to cover the integrity, confidentiality and availability of data, and that such controls are regularly assessed and tested. As the Hong Kong Monetary Authority declared, “The Board and Senior Management are expected to play a proactive role in ensuring effective cybersecurity management.”

A cybersecurity strategy can help your institution to deliver the right response to these mounting regulatory demands by harnessing:

- Privacy by Design – which should be embedded in any digital strategy. A well-constructed privacy program recognizes the need to comply with regulation while also ensuring privacy does not become a blocker to digital innovation.
- Financial services regulatory compliance controls – which should be embedded in the organization’s operational risk agenda. However, institutions should avoid compliance for compliance’s sake, as this can leave the organization exposed, with a sub-optimal cybersecurity framework.

Cloud management

Regulation, especially privacy regulation, is increasingly placing liability on financial services institutions to manage and protect data residing with a third party. In this case, don’t assume that third party cloud providers have adequate security controls.

To safeguard your digital assets and build trust with customers:

- Ensure identity and access management is in place in the cloud ecosystem.
- Build cloud-aware controls that are independently tested and verified by a certifying body.
- Invest in a trusted design, execution and certification of your cloud ecosystem.
## Process and technology controls

### Applications

As the number of applications running in distributed or untrusted (third party) environments continues to rise, so does the frequency, sophistication and severity of security breaches.

<table>
<thead>
<tr>
<th>Key risk area</th>
<th>Suggested response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design</strong> — security may not be part of the initial functional design, creating significant security flaws that enable fraud</td>
<td>Embed security as part of initial design by identifying business use cases, developing threat models and their associated controls</td>
</tr>
<tr>
<td><strong>Source code</strong> — malicious code and/or flaws in the code (e.g., cryptography) may assist future attacks on the application</td>
<td>Source code reviews are essential throughout the systems development life cycle, using both manual and automated techniques</td>
</tr>
<tr>
<td><strong>Application vulnerabilities</strong> — common vulnerabilities (e.g., developer ‘back doors’) may be overlooked in the haste to get to market</td>
<td>Ongoing application vulnerability assessments prior to production to identify and remediate any vulnerabilities</td>
</tr>
<tr>
<td><strong>Application integration</strong> — other systems that the application interacts with in the ecosystem may be insecure</td>
<td>Ensure source and target systems are not a source of systemic risk, especially vulnerable legacy applications</td>
</tr>
<tr>
<td><strong>Perimeter security devices</strong> — are normally inadequate and should not be relied on</td>
<td>Implement application level security, such as Web Application Firewalls</td>
</tr>
</tbody>
</table>
| **Application Programming Interfaces (APIs)** — open up digital assets to a broader ecosystem of partner and customers, but they also increase digital risk through, identity, parameter and man in the middle attacks | Take a structured approach to API security that builds in base line controls, including:  
  - Turning on encryption for API communications  
  - Checking incoming data against expected values in your API related data schema  
  - Extending threat detection to specifically incorporate threats associated with APIs |
Application distribution

Not all publically available application stores vet applications for authenticity before making them available for download. Cyber criminals continue to repackage code within legitimate applications or simply create new applications that purport to contain new functionality – and customers find it very difficult to determine legitimate from false updates. To help manage this risk:

- Ensure you have incident response plans in place to deal with fake applications – commercial providers offer ‘take down’ services with agreed SLAs
- Monitor the application stores that your applications sit in for fraudulent versions
- Educate your customers and staff about cyber awareness

On-boarding customers quickly and securely

Your institution faces a challenging trade-off between wanting customer registration for digital services to be fast and easy, and ensuring strong proof of identity. It also needs to continue to perform identity checks throughout the customer life cycle – from both a security and user experience perspective. To smooth this process, while keeping it effective:

- Analyze how to leverage existing authoritative user stores for current customers signing up to new digital services
- Consider physical registration for potential customers who have no history with you today – in some jurisdictions, a degree of physical in-person verification is already mandatory
- Include customer identity lifecycle management in the base-level service design – otherwise, when credentials expire, re-proving identity will become a major customer impost

Authenticating customers

Insufficiently complex passwords and the increasing sophistication of cyber criminals make customer authentication credentials vulnerable to theft. Even multi-factor authentication may not be effective without complementary controls. For higher value and risk transactions, consider ‘step up’ authentication, where additional user authentication credentials are required before the transaction request is approved.

Beyond data encryption

- **Data in transit** – as transaction data moves between a customer’s device (tablet, PC, mobile) and your systems it provides an ‘attack surface’ for cyber criminals to both steal credentials and direct transactions to fraudulent sites. However, encryption for transaction data in transit is no longer sufficient as a control, as attackers can now gain entry from an authenticated end point device. Make sure you implement framework controls that incorporate the end point device.

- **Data at rest** – should be encrypted, as it provides a static attack surface for malware, hacking and inappropriate internal user access. However, you also need to consider the processing overhead of encrypted data. In parallel, try using internal user access management frameworks to provide assurance over appropriate employee access to customer and organizational data.
Third-party ecosystem management

Digital strategies in financial services are increasingly opening up your enterprise boundary to third parties, such as brokers, fund managers or payment providers. This introduces potential systemic risk from the ecosystem. Third parties often have weaker security controls than your institution, creating a ‘back door’ for attackers to gain access to the organization.

Third-party risk management framework

You need a risk management framework overarching your digital ecosystem to help ensure you can:

- Identify all flows of data to and from third parties and all system and application access points
- Conduct due diligence reviews of third parties’ cybersecurity controls
- Embed contractual obligations
- Define specific requirements for your third parties
- Secure transfer of data and access points
- Gain regular assurance over third parties

Proactive monitoring

Cyber attacks on financial services providers are becoming increasingly sophisticated and targeted, with attacks occurring over a prolonged period of time. The truth is that institutions cannot and will never be able to prevent cyber attacks completely. As former FBI Director, Robert Mueller, says, “I am convinced there are only two types of companies: those that have been hacked and those that will be.”

This is because technology advances so quickly that IT defences are continually playing catch-up, with new malware such as Advanced Persistent Threats that can sit unnoticed on your network slowly and patiently sending out confidential data.

To identify fraudulent or malicious patterns and apply appropriate controls, fraud and transaction monitoring should be implemented, based on anomalous behavior detection. Deploying security analytics combined with tailored threat intelligence feeds can also help you to identify future threats and manage them before they cause damage.

Service availability

Cyber attacks increasingly present a risk to the service availability of digital channels, with the development of targeted Malware that degrades or takes services off line, in addition to Distributed Denial of Service attacks. Non-malicious cyber threats can also impact your digital service availability; such as lack of a governance process to renew SSL certificates.

To address some of these issues, a number of service providers offer anti-Distributed Denial of Service (DDoS) as a managed service. You should also ensure you have comprehensive incident response plans in place and test these regularly against different scenarios through drills or simulations.
Incident response

An attack or a data breach is an inevitability. No cyber risk management framework can be 100% effective in the face of a fast-paced, continuously evolving threat environment. Institutions that are not prepared to respond to and manage a cyber incident may face legal, regulatory, brand, market share and stock price impacts.

You need comprehensive Incident Response Plans (IRPs) in place, involving: PR, Regulatory, Legal, Operations, Risk Management and Digital Business units. Test your IRPs regularly through drills across multiple threat scenarios matched to your risk profile, and feed the lessons learnt back into the plan.

Social and mobile management

Social media is an important direct channel between companies, employees and customers, delivering collaborative power to innovate and share information instantly. However, it can be a double-edged sword in the hands of disgruntled customers, activists and malicious cyber criminals.

Make sure your organization has a holistic social media strategy, integrated and coordinated with marketing, branding and internal and external communications.

To protect your brand image, establish awareness training so employees understand the steps they need to take to protect your organization when interacting with customers on social media – as well as their own personal brand and reputation.

Education and user awareness

Process and technology controls alone cannot provide an effective cybersecurity strategy. Given the increasing sophistication of phishing and social engineering attacks, people are both the largest source of vulnerability and the strongest line of defence in any leading cybersecurity strategy.

This is why education and awareness must form a continual part of your cybersecurity strategy. Using a slow and steady approach, educate your customers, employees and third parties on the common tools and techniques used by malicious actors to use them as a point of entry into your organization.
Let’s talk cybersecurity

Is your business strategy fit for a digital world?

For EY Advisory, a better working world means solving big, complex industry issues and capitalizing on opportunities to deliver outcomes that grow, optimize and protect our clients’ businesses. We’ve shaped a global ecosystem of consultants, industry professionals and collaborations with one focus in mind – you.

Anticipating and now actively defending against cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities.

We then work with you to co-create more innovative answers that will deliver the solutions you need. Together, we help you deliver better outcomes and long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.

Jeremy Pizzala (Author)
Asia-Pacific
Financial Services
Cybersecurity Leader
+852 2846 9085
jeremy.pizzala@hk.ey.com

Paul O'Rourke
Asia-Pacific
Cybersecurity Leader
paul.o'rourke@sg.ey.com
+65 6309 8890

Anthony Robinson
Oceania Financial Services
Cybersecurity Leader
anthony.robinson@au.ey.com
+61 2 9248 5975
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2015 EYGM Limited.
All Rights Reserved.

APAC no. 00000339
ED 0616
S1528272

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

www.ey.com