Cybersecurity Fortification Initiative (CFI) infrastructure whitepaper
Recently, Cybersecurity Fortification Initiative (CFI) have been a hot topic in the Hong Kong banking industry and financial institutions are working very hard to comply with the initiative. During the exercise, financial institutions are going through a cycle which Deloitte define as Secure, Vigilant and Resilient to reassure the requirements are being addressed. However, it is also important to look at it from the operation side by implementing necessary controls and technologies.

**Technology Risk Framework**

Deloitte's technology risk framework incorporates key cybersecurity areas and is built on industry leading practices and regulatory expectations. It allows our clients to take stock of current capabilities to manage cyber security risk.
Network is the fundamental element of the business environment and it is important to secure and set as the priority.

Improvements in cybersecurity posture are also possible as network segmentation can be used to reduce the risks and impact of cyberattacks. By taking a pragmatic approach to introduce network segmentation, financial institutions can minimize business disruption and reap benefits, such as limited exposure after an intrusion, reductions in lost productivity, remediation costs, and reputational damage from actual loss of personally identifiable information (PII) or financial data. As part of a layered security philosophy, network segmentation enables financial institutions to survive intrusions and minimize or even prevent successful data breaches. In the end, this allows for a speedy return to business as usual.

Network segmentation is a "tried and true" technique that has been implemented through the years to address an assortment of issues in IT infrastructure environments. Network segmentation ultimately leads to improved availability of the entire network by localizing the impact of faults when they do occur. Extending this concept to cybersecurity, network segmentation can restrict lateral movement of malware or malicious actors if or when a PC or server is compromised. With network segmentation, the cyber attacker is contained to a localized portion of the network to minimize the opportunities to find valuable information or resources. Network segmentation is a key element in a layered defense model for cybersecurity. However, it requires collaboration among business and technology leadership in order to be adopted across an organization.

Current state
In spite of the near universal consensus on the value of network segmentation for improved cybersecurity posture, actual implementations are still rare on internal networks. Many financial institutions have essentially "flat" networks, as far as security is concerned. This puzzling inconsistency between the mindset related to and the practice of network segmentation is actually easy to explain. For many years, the primary concern was to protect the network perimeter. The outside was "dirty" and the internal network was "clean". The objective was simply to keep the undesirable traffic out.

Moreover, there was and still is an incomplete knowledge of applications and traffic flows inside the network.

Consequently, this necessitates an open internal network to allow communications to occur freely in support of business applications. This places too much reliance on the legacy controls at the network perimeter of the financial institution, which are not entirely effective against the sophisticated attacks of today.
Challenges to reach the desired state
Financial institutions have complex networks that encompass remote offices, retail branches, campus sites, third-party partners and e-commerce environments and there are concerns over the introduction of internal network segmentation for cybersecurity.

- Incorrect or incomplete identification of required traffic flows would lead to potential disruptions to business applications.
- To properly implement network segmentation in a "brown field" environment is a significant undertaking that will require cooperation from stakeholders in the security, application development, network, compute, storage and business functions.
- The creation of a governance process for new or modified applications will be required to sustain the network segmentation.
- Updates to the security policies will be needed as traffic patterns change due to movement of infrastructure components, modifications in applications themselves, or the introduction of new applications.
- There is a cost in both capital and operating expenses associated with the initial deployment of segmentation gateways as well as with the ongoing management of those devices.

Business drivers
Perimeter network security alone is not completely effective against the increased sophistication of advanced persistent threats and the multiple attack vectors facing financial institutions. In spite of the challenges associated with network segmentation, there are some key business drivers in support of it.

- Minimize the time, effort, and resources associated with audits (e.g., PCI DSS) by reducing their breadth through compartmentalizing related resources on the network.
- Limit exposed resources to constrain cyber attackers ability to find critical data or intellectual property even if they gain a foothold in the network.
- Prevent the movement of malware from end-user systems to more sensitive systems and data center resources.
- Supplement the capabilities of perimeter security controls with another layer of defense on the interior of the network.
- Avoid or minimize the lost productivity, remediation costs, credit monitoring costs, reputational damage, and class-action lawsuits in the aftermath of data breaches.
Mechanics of network segmentation

Network segmentation cannot be achieved in a vacuum. The involvement of stakeholders across multiple disciplines, including application architects, network architects, business application owners and information security personnel is essential. Together, this cross-functional team needs to take several steps to actually segment the network.

• Identify applications, including their traffic flows and dependencies.
• Architect the segmented network.
• Construct security policies.
• Enable additional security capabilities.
• Continuously monitor and update.

Practical approaches

Implementing network segmentation is a non-trivial effort in an existing environment. However, this should not deter a pragmatic approach to adopting some degree of segmentation in the internal network. The ideal would be to achieve a "Zero Trust" network, as defined by Forrester. Every organization will need to determine how much network segmentation is appropriate for its situation. With that in mind, here are some practical considerations for introducing this concept to an internal network.

• Select low-risk environments as proofs of concept. Compartmentalizing all servers used for an application test environment would bring minimal risk to the overall business.
• Deploy initially in locations with easier physical or topological considerations. The access layer of the network, where end-users reside, only transports data required by that population.
• Separate the data center from the portions of the network where end-users reside. This is essentially providing north-south controls over traffic from the entire user population to the services in the data center.
• Leverage cloud initiatives to segment resources. New private or public cloud projects provide an ideal situation to impart controls over application and data flows inside and out of those environments.
• Prioritize which data and workloads to segment. Any portions of the network that warrant special consideration due to audit or regulatory concerns should be prioritized.
• Establish governance for new applications or modified workloads. Visibility and knowledge of new or changing traffic patterns is required to adjust the security policies accordingly.

**Conclusion**

Network segmentation has been a boon to network performance and availability over the years—enabling effective use of business applications. In a cybersecurity context, network segmentation will protect financial institutions from being completely exposed after an initial penetration by malicious actors. Containing the intrusion to a portion of the environment reduces the overall risk to the institution. Implementing network segmentation across the entire estate is a major undertaking. However, a practical approach to introducing this in a controlled and strategic manner that is consistent with the institution’s overarching security architecture will minimize any potential business disruptions. Network segmentation adds another layer of protection that will partition the enterprise network into manageable, secure segments to reduce the attack surface, limit data exfiltration, and reduce the scope of audits and compliance.

With the collaboration between Deloitte and Palo Alto Networks, which played an important role in providing cyber threat intelligence and help to prevent breaches to many financial institutions, it is no doubt that this consortium is one of the best choices with which to engage. Beyond network segmentation, this partnership can provide additional solutions to elevate the cybersecurity posture of your financial institution.
Deloitte and Palo Alto Networks

Thomas Lee
Partner, Risk Advisory
Deloitte China
Tel: +852 2852 1931
Email: thomalee@deloitte.com.hk

Stephen Chan
Director, Risk Advisory
Deloitte China
Tel: +852 2238 7346
Email: stchan@deloitte.com.hk

Wickie Fung
General Manager, Hong Kong & Macau
Palo Alto Networks
Tel: +852 9644 8330
Email: wfung@paloaltonetworks.com

David Wong
Regional Sales Manager
Palo Alto Networks
Tel: +852 9106 9906
Email: dwong@paloaltonetworks.com
About Deloitte Global
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte China
The Deloitte brand first came to China in 1917 when a Deloitte office was opened in Shanghai. Now the Deloitte China network of firms, backed by the global Deloitte network, deliver a full range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. We have considerable experience in China and have been a significant contributor to the development of China’s accounting standards, taxation system and local professional accountants. To learn more about how Deloitte makes an impact that matters in the China marketplace, please connect with our Deloitte China social media platforms via www2.deloitte.com/cn/en/social-media.

About Palo Alto Networks
Palo Alto Networks is the next-generation security company, maintaining trust in the digital age by helping tens of thousands of organizations worldwide prevent cyber breaches. Our innovative security platform with game-changing technology natively brings network, cloud and endpoint security into a common architecture. By doing this, we safely enable applications, users and content, deliver visibility, automation and control, and detect and prevent threats at every stage of the attack lifecycle, so organizations can securely and efficiently move their businesses forward.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.