FROST & SULLIVAN

Risk and Cyber Security – Awareness, Action and Involvement

Examining enterprise attitudes and initiatives towards cyber security, and the risks that remain unaddressed

A Frost & Sullivan Growth Insight
commissioned by Forcepoint

Forcepoint

Contents

1.0

Ushering In The Digital Transformation Era

The technology industry has been hearing the word "transformation" in every other boardroom, on the first page of every second whitepaper, in every imaginable permutation and combination.

The business case for transformation

The technology industry has been hearing the word "transformation" in every other boardroom, on the first page of every second whitepaper, in every imaginable permutation and combination. The hype surrounding digital transformation has had a boy-who-cried-wolf effect - almost muting the very real urgency and impact of this structural shift. There's no single reason pushing this transformation...oh, wait. Actually, there is. The customer is at the very center of every experience. Today's digital landscape has put the customer firmly in the driver's seat - through the power of highly connected networks, social media, and a feedback-driven consumer culture, creating a customer-first service model means a revenue-rich business.

The big challenge for C-level leaders is being able to separate out the conceptual from the tactical. Business leaders are inundated with massive amounts of information, advice and conflicting business priorities: when is the right time to buy into a new trend? What is the most practical way to transform a business? How do you spot a critical risk from a necessary compromise?

Getting these decisions right separates successful businesses from the ones breathlessly trying to catch up in the race to be more agile, customer-centric and insights-driven. And this means bringing in tools to allow all the below:

Personalising experiences on a large scale by moving to unified platforms that allow consolidating customer touchpoints. Traditional business models run different operations on many fragmented media channels - moving to a single unified platform allows for supporting seamless experiences across every customer touch point.

Collaboration that easily connects people, systems, and information – enabling visibility into every part of the customer journey. C-level executives who succeed at implementing this correctly are learning that this is the answer to some of their biggest challenges - providing a reliable and consistent customer experience and curating top talent.

Allowing easy access to all the data needed to make important decisions - Technologies such as the internet of things (IoT), artificial intelligence (AI), big data and machine learning (ML) are powering business decisions by boosting competitive insight efficiencies. This hasn't always been the case - the past few decades have been missed opportunities for insights and analytics which were always forced into the background. Today, next generation technologies have pushed the insights function right into the foreground to feed into core business strategies.

Meeting expectations of the modern workplace - Historical infrastructures, solely on-premises networks and self-managed storage frameworks belong to the past. Businesses that don't embrace modernity are left behind, appear redundant in the eyes of customers, aren't able to retain key talent, and aren't able to partner well because they aren't compatible with modern technologies. With all these changes, C-suite executives are having to reimagine traditional approaches to security and innovate new ways to leverage data for growth.

The transformation lifecycle: drivers, enablers, goals, and challenges

When examining the drivers, enablers, and goals of transformation, the answers are easy – the business landscape is changing, and organizations that rely on archaic forms of making and executing business decisions are finding their customers churning faster, their platforms unable to scale, and their service models seeing margins getting thinner. Today, the C-level executive needs to elevate the customer experience and drive change.

> Transformation is a technology enabler. It opens the door to innovation and opportunities that didn't exist before and allows reshaping product and service offerings to be more agile.

> AI, automation, big data, and IoT are examples of disruptive tools that are helping organization owners better understand their market, their consumers, and their competitors.

> A great example of a digital accelerator is the use of microservices: the software design architecture that breaks down the traditionally monolithic platform model. A long term goal of most business-critical software products, enabling microservices would make it significantly easier to handle changes in business direction or consumer demands by allowing teams to develop, deploy, test, and change each service independently.

On the other hand, walking through the challenges of digital transformation is a bit of a cart-before-the-horse dilemma. Are these challenges genuine results of transformation? Or do they stem from overzealous planning where businesses bring in disruption before first laying down the right groundwork?

From Frost and Sullivan's 2019 Asia Pacific (APAC) Risk & Cybersecurity study for Forcepoint, 95% of respondents have embarked on their digital transformation journey, out of which 65% are concerned about cyberattacks thwarting these transformation efforts. And these aren't just numbers - consumer favorite ASEAN brands like Sephora, Uber, Toyota and Singapore Airlines have suffered the logistical and PR nightmares of losing customer trust in large data breaches within the past year alone. Every layer of digital transformation is another layer vulnerable to security attacks. For digital-ready enterprises, the security checklist essentially falls into one of the three must-have buckets below:

Ensuring compliance against regulations:

Organizations are starting to consider where their products are implemented and where their data is stored, in terms of cybersecurity risks and regulations. And with regulations evolving by country and by region, it's challenging to ensure compliance over time.

Keeping your data from risk:

Employee-caused security breaches remain one of the top causes of cyber risk, whether intentional or unintentional. Despite this, enterprises are still not consistently laying down security awareness training programs, or incident response processes. It points to a need to create additional oversight and control, but without slowing down transformation or business continuity.

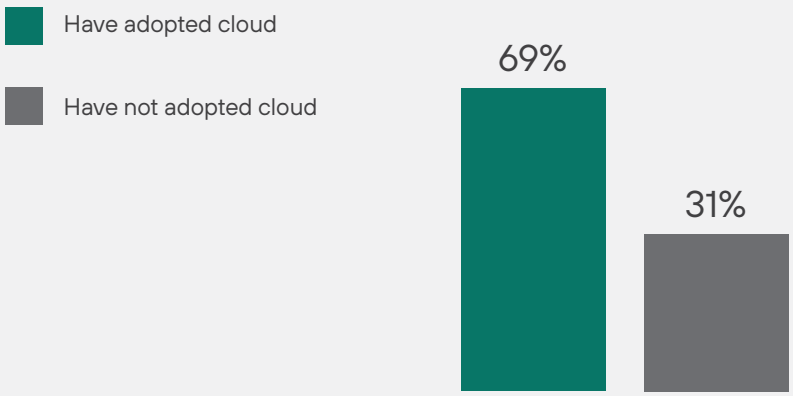
Enabling partnership safely:

Enterprises have a need to share data with 3rd parties and external partners. At times, this means enabling collaboration in tools that aren't core to the business. Without doing their due diligence in ensuring security, particularly in cloud-based tools, the business can be exposed to additional risk. Taking an approach that is comprehensive to partnerships does wonders in minimizing the attack surface, particularly when an organization's critical data or personal data is involved.

2.0

In the Spotlight: The Age of Cloud-driven Business Revamping

Figure I: Overall Cloud Adoption Technology Australia, India, Singapore and Hong Kong



Digital transformation is only half the story - the epilogue of which is the cloud journey. The same study by Frost & Sullivan revealed that 69% of enterprises are currently using cloud technology.

Cloud service models in the age of business transformation

Digital transformation is only half the story - the epilogue of which is the cloud journey. The same study by Frost & Sullivan revealed that 69% of enterprises are currently using cloud technology.

Shifting service models into the cloud was the first true enabler that allowed businesses to understand their market better, and then respond faster to those learnings. The change in the knowledge-to-action timeline was phenomenal - reducing it from days or weeks, instead of a slow, bureaucratic, disconnected process of convincing the entire stakeholder chain at a glacial pace to respond to a new trend that, by then, was already obsolete.

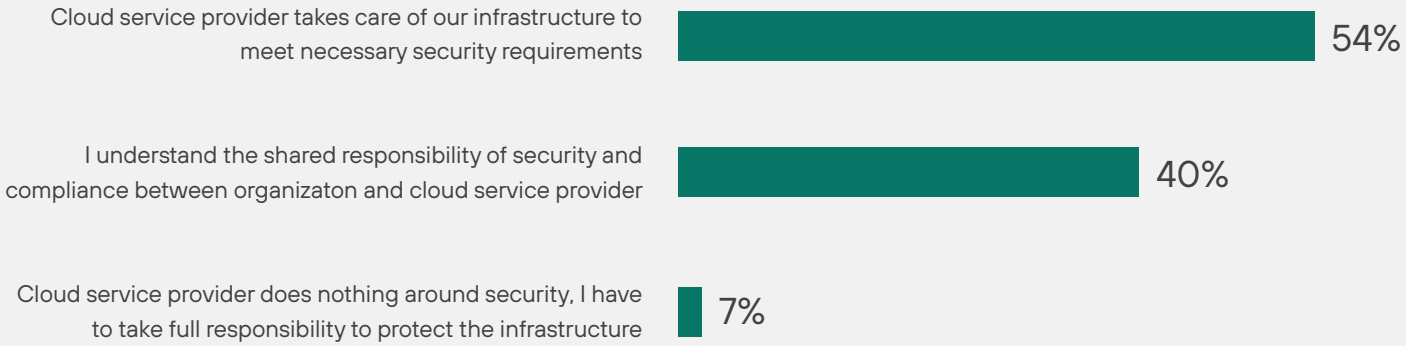
Cloud models have allowed for a wide expanse of operational efficiencies:

• Cloud service models (Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service) have shaved off dozens of steps with both delivering applications to end-users, as well as deploying dynamic web applications.

• The benefits of these models, when implemented cautiously and strategically, have enabled C-level executives to realize improvements in key success metrics such as scalability, operational efficiency, and increased profits versus traditional data center deployments.

> Based on the Frost and Sullivan study, 55% of enterprises are at risk, either by having encountered a security incident in the past, or by not setting up any necessary checks to rule out security breaches within their environments.

Figure 2: Common Misconception of Responsiblity in Securing the Cloud Environment in Australia, India, Singapore and Hong Kong



Over the past 10 years, the cloud has gone through a full cycle of disruption: learning through growing pains, finessing the right risk-to-reward balance, and finally reaching a level of maturity that enables easy access for organizations spanning all industries and scales. Most importantly and when implemented correctly, the cloud transformation allows companies to focus on their core business, instead of always finding themselves having to be their own IT delivery provider.

Curating a security-first mindset in the cloud era

Based on the Frost and Sullivan study, 55% of enterprises are at risk, either by having encountered a security incident in the past, or by not setting up any necessary checks to rule out security breaches within their environments. Adding to this is a common misconception - 54% of enterprises studied think that the responsibility of securing their cloud environments falls entirely under the purview of cloud service providers. Since this is not always the case, the gates are often left unguarded, making enterprises an easy target.

• The **consequences of a security breach** are significant: legal repercussions, loss of customer trust, and severe non-compliance penalties. Security management and access management need to be handled by the enterprise itself, along with the responsibility of appointing the right organizational roles to research and action frameworks to meet global security regulations.

• The **drivers of cloud security**, too, are evolving with the speed of growth in data volumes and storage needs. The vast landscape of connected devices in today's enterprise networks means that even a minor breach into a single unprotected point means a potential security breach to the whole network. Additionally, advanced data analytics and information storage infrastructure makes it easy to collect and analyse large sets of sensitive data in very little time. As a result, massive, rich datasets are being collected and stored by businesses, doubling up as an easy target for cybercriminals who can exploit vulnerabilities and easily steal critical data and IP including the customer data.

Enter the shared responsibility model. This is a cloud security blueprint of sorts, which serves as a mutually understood best practise in cloud environments. While different cloud providers may define and enforce this in slightly varied ways, the base remains the same: this model outlines two key areas of security responsibility: firstly, the pieces that the cloud provider is responsible for; and secondly, the areas that the organization itself is responsible for. Under this, organizations are still responsible for the security of their data in the cloud, while cloud providers are responsible for the security of the cloud itself - the compute, storage, and networks that support the public cloud.

This calls for C-level leaders to give more thought and planning to considerations like:

From a risk-based perspective, does my data need to go up to the cloud?

There is no single answer - this depends on each application, service, and type of consumer demand. Additionally, the follow-up question here is: what data, specifically, needs to go into the cloud? These considerations revolve around a combination of using the right identity and access management platforms, training security operations, IT, and development teams to make sure the right people have access to data at the right time, that security policies are properly updated on the cloud, and that a centralized approach is applied on to compliance management (whether it's GDPR, HIPAA, or country-specific data privacy and security regulations).

How do I automate processes to move to a preventative security posture?

Security-first companies are starting to build cybersecurity right into their organizational fabric: into their customer relationships, manufacturing and production lines, and vendor procurement processes. The most successful tactics leverage threat intelligence and quantitative analysis for risk assessment; building cybersecurity right into the business value chain and embracing innovation, and agile technologies including but not limited to robotics, cloud, and DevOps.

How do I build a culture of continuous improvement and security?

Security teams within enterprises are finally focusing on one of the most common sources of risk - their employees. This revolves around making employees feel like partners, encouraging them to be collaborative and vigilant, and working together and with underlying security tools to create culture-aided processes around threat awareness and detection. Tools may need to implement coaching or prompting as data security policies change, so that they provide safeguards while tasks may be in process and employees may be distracted.

3.0

Cyber Risk Exposure

From the same study conducted for Forcepoint: 35% of enterprises surveyed have had an adverse security incident in the last 12 months.

Security considerations in the age of digital transformation

With digital transformation having moved from being just a buzzword to a necessary, definitive reality in today's modern organizations, new catalysts are driving today's risk landscapes:

Wider attack surface areas

The number of applications and the amount of data that is now in the digital realm is exponentially higher. And with this, hackers have more opportunities. With more targetable points of entry than ever, security professionals have to work harder and smarter to effectively manage their threat perimeters.

Increasingly intelligent attacks

Hackers are getting more sophisticated, with smart, modern technologies acting as a catalyst. Advanced technologies (such as artificial intelligence) that are available to security professionals are also available to cyber criminals.

A tug of war between business agendas and security protection

The only constant is change - businesses always have to stay competitive alongside rivals who are always evolving, adding new features and creating churn. In response, new products and services need to be rolled out faster, which sometimes leads to security shortcuts being taken. Strategic businesses do well when they position the CISO role as one of an educator and C-level champion to curate a security-first mindset and help leadership make informed decisions around risk trade-offs.

From the same study conducted for Forcepoint: 35% of enterprises surveyed have had an adverse security incident in the last 12 months. Within this research, a few common blind spots emerged –security incidents that have a high level of impact but are simultaneously faced with long recovery times, a combination that leads to significantly damaging business impact. In order of magnitude, these include loss of intellectual property, online brand impersonation, unauthorized access to user accounts, and data exfiltration; the list grows longer with more and more sophisticated attack patterns.

The transformation divide: Examining market gaps separating the business from the technology

Singapore, Hong Kong, India and Australia - All have their unique advantages in security-readiness, digital transformation efforts, and government-backed regulatory frameworks for cybersecurity. However, Frost and Sullivan's security research within these four markets has revealed critical market gaps spanning both technology and management challenges:

Talent Shortage

Technical skills shortages with a lack of adequate, qualified talent to fill the huge and ever-growing job market within cybersecurity. All four regions are seeing low headcounts for security professionals, where most of the growth at the moment comes from workers transitioning from related sectors instead of new graduates entering the workforce. To combat this, universities and vocational institutions have been working towards launching new cyber security courses and degrees.

Nascent R&D

Cyber security research and development in regions like India and Australia are still in their nascent, fledgling phases, and need more public funding and industry collaboration to properly fuel innovation.

Shrinking security budgets

Security champions within organizations are still fighting to communicate security needs and risks effectively to board members, a challenge that is exacerbated by the constant fight for budgeting. For instance, 27% of enterprises in Hong Kong reported that their security budgets were reduced by their management teams.

Room for growth with regulatory support frameworks

Lastly, there is a lack of adequate support infrastructure for smaller security business and startups. While these organizations might have strong best-of-breed approaches to focused problems, they often lack the ability to integrate with existing systems. This limits the potential to scale and provide the support needed for client-side expectations that larger enterprises find easier to deliver.

Key takeaways for businesses

Simply put, enterprises cannot afford to stay in a static state of security transformation. Every stakeholder in the ecosystem - suppliers, partners, and end-customers - now demands a higher level of security compliance. By not addressing the issue, enterprises can lose out on important sources of revenue and industry recognition, which is propelling competitive businesses to get their security strategy straight.

Having a new model for security relies almost entirely on being able to set up defences way before cybercriminals can target and exploit a new vulnerability, instead of waiting for new threats to inform detection strategy and constantly being in firefighting mode. Here are some initial steps to begin laying out clear groundwork for a dynamic security posture:

Safeguard what you know is valuable. This points to implementing next-generation security technologies such as next-generation firewalls (NGFWs), next-gen endpoint security, identity, and access management (IAM) and multi-factor authentication (MFA), and using these techniques in conjunction with a comprehensive breach response plan. There are technologies available to make these toolsets easy to manage – and even apply Firewall policies, IAM, and MFA across the entire environment – whether you are on-premises or in the cloud.

Adopt a security framework built for the modern environment. Do not rely on perimeter defences to catch today's advanced and unknown threats. If organizations always rely on the wait-and-see approach, they constantly have to stay in the mode of clean-up and damage control, draining time, money, and resources. Instead, security-first enterprises need to adopt a more proactive, zero-trust strategy.

Set up proactive frameworks of continuous risk assessments, strict access management policies for business applications, vulnerability testing, and a failsafe disaster recovery strategy.

Educate your workforces about safe cybersecurity practices, security awareness policies, and how to identify and correctly report malicious threats.

4.0

The Forcepoint Blueprint: A Human-centric Approach to Modern Cybersecurity

How can enterprises bring their digital visions into reality when their people, data and infrastructures are moving outside of their control?

How can enterprises bring their digital visions into reality when their people, data and infrastructures are moving outside of their control? As enterprises disrupt their traditional ways of working, it often leads to increased productivity and profitability. But it also creates an opening for hackers and nation-state adversaries to take advantage of this transition to damage businesses. Whether it is stealing intellectual property, phishing for personal data, or causing maximum business disruption, the stakes have never been higher for enterprises.

As enterprises shift more applications and services from on-premises to the cloud, their existing infrastructure-centric security is a mismatch to securing user access and data in this 'wherever they are' cloud environment.

Today, 90% of breaches are the result of a compromised identity – compromising user access to expose critical data and intellectual property. When a "standard" point product registers authorised credentials and allows access, its job is done. However, what if that individual, using accurate credentials, is not a real employee, but a hacker in disguise? The legacy cybersecurity approach will allow an attacker to access an organization's network. It is nearly impossible to defend against hackers who have compromised good employees by illicitly "owning their systems". Good employees can make mistakes that unwittingly cause data leakage, creating just as much damage as disgruntled employees who may not have the best intentions.

It becomes critical to understand the behaviors of all users—employees, customers, and partners—as they interact with data and systems. Modern cybersecurity addresses this by recognizing that people are the new perimeter. This means enterprises must change the focus of today's cybersecurity approach to the two constants: the people on their network and the critical business data they access daily.

Risk-adaptive, behavior-based cybersecurity

Forcepoint helps organizations focus on users and data – identifying and mitigating compromised access before the breach happens. It has instrumented its security capabilities to deliver automated mitigation of the risk by integrating behavior analytics across endpoint, network, and cloud. It begins by understanding the behavior of users interacting with data on the network, identifying where risk lies at the user level. It quantifies the risk in real-time and uses that risk to take action in an automated fashion through the implementation of risk-adaptive protection.

This human-centric security approach allows enterprises to recognize abnormal behaviors and ultimately stop bad things from happening while freeing the good. Security leaders can quickly and continuously assess the potential of compromised user risk and take action as the risk level goes up.

Modern cybersecurity must put people and data at the center of its design thinking, and this new multi-dimensional world isn't going to change any time soon. By 2020, 73% of enterprises will run almost entirely on software-as-a-service. Forcepoint is uniquely positioned to capture this industry shift towards "as-a-service" model. Through its behavior-based converged security platform, Forcepoint provides an extensible foundation for delivering integrated security solutions to enterprises and government agencies as a cloud-first, hybrid-ready service.

Forcepoint's new capabilities include Dynamic Edge Protection and Dynamic Data Protection. These solutions present a very real opportunity for customers to derive the benefits of digital transformation, allowing them to accelerate business growth and desired business outcomes.

Forcepoint Dynamic Edge Protection

It combines Forcepoint's next-generation web and network security and connectivity to enable cost-effective network protection against advanced threats, while securing remote users with zero-trust, direct-to-cloud connectivity. Using Forcepoint Dynamic Edge Protection, organizations can garner 50% reduction in cost of branch office IT personnel and Network.

Forcepoint Dynamic Data Protection

It combines Forcepoint's industry-leading DLP capabilities with a behavior-based analytics capability to deliver risk-adaptive, unified data, and intellectual property protection for hybrid and multi-cloud enterprises. Dynamic Data Protection establishes a "normal" baseline of user behavior and applies a range of automated security countermeasures based on fluctuations in a user's risk score, all without administrator intervention.

Cybersecurity today is a business-critical issue and, for an organization to win against the attackers, it requires security programs that focus from the top down, not the bottom up. In placing people and data at the center of design thinking, enterprises and government agencies can secure their digital transformation journeys for long-term business success.

Global technology partner ecosystem extends risk-adaptive protection

Forcepoint has been strategically investing in the creation of a broader technology partner ecosystem that enables customers to achieve their digital transformation outcomes. Forcepoint's global technology and strategic alliances span areas including identity and access management, data security, discovery, classification, cloud infrastructure and cloud apps, security operations, and behavioral analytics.

Through its partner ecosystem, Forcepoint enables customers to simplify collaboration to create an integrated security stack that offers frictionless, automated and hybrid solutions. Some of the key technology alliances include AWS, IBM Security, Microsoft, Citrix, Boldon James, Ping Identity, Seclore and more.

Find out more at:
www.forcepoint.com/platform/technology-partners

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models.The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com

ABOUT FORCEPOINT

Forcepoint is the global cybersecurity leader for user and data protection. Forcepoint's behavior-based solutions adapt to risk in real-time and are delivered through a converged security platform that protects network users and cloud access, prevents confidential data from leaving the corporate network, and eliminates breaches caused by insiders. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of enterprise and government customers and their employees in more than 150 countries. www.forcepoint.com