CGI

Experience the commitment®

EXECUTIVE PAPER

Data Security Risks and Cyber Resilience in a Hyperconnected World

cginederland.nl/cybersecurity

Executive summary

In the last two decades, the technology revolution has changed the way we all go about our business. While offering opportunities for innovation and productivity, the cyber era also presents new risks and challenges.

In this executive paper, we address the complexity of cyber data risks and the shared responsibilities of all entities in the cyber data ecosystem to protect data and respect privacy laws.

The complexity of this topic is divided in 5 sections:

- Data security risks in a hyperconnected world;
- The cyber data ecosystem;
- Data strategies in the cyber data ecosystem;
- Data privacy regulations in the cyber data ecosystem
- Executive responsibilities in the cyber data ecosystem.

Many leaders in business and government realize that for the world‟s economy to fully benefit from technology innovation, a robust, coordinated system of global cyber resilience and data privacy and protection is essential to effectively mitigate the security risks of a hyperconnected world.

Regulation in the data privacy arena is far from static. As data flows between countries with disparate data protection laws, organizations need to ensure the security of their customer and employee data through regulatory compliance and due diligence. However, multinational organizations often find disparate data privacy laws exceedingly challenging.

Many sophisticated U.S. businesses are sometimes shocked to learn of the significant regulations for personal information in foreign countries, particularly in the European Union and how these impact cross-border data flows. Businesses are well advised to fully understand internal data flows and conduct a legal assessment of not only domestic privacy law compliance, but also foreign operations and cross-border data transfers. In the section called *Data privacy regulations in the cyber data ecosystem,* we will drill down in detail with respect to the global geographical differences in privacy protection.

There is no single best practice or uniform strategy in general for decisions about data protection. As discussed in this paper, laws and regulations in countries vary in their nature and level of protection. Countries regulate in different ways the type of data you want to store as well as storage locations.

Data that is not subject to laws or regulations or any other type of governmental oversight can be protected and stored as the owner sees fit. However, even if there are no legal restrictions, customer and other stakeholder interests play an important role in decisions about data protection and localization.

The hyperconnected world has removed the traditional security data perimeter as organizations adopt cloud, mobile, social and other borderless technologies, and invest in third-party business relationships. Data protection and privacy laws and regulations address the risks of data flowing across national boundaries through these new technologies.

Based on the data security risks in a hyperconnected world, executives have the responsibility to consider their organization‟s current data security protection and cyber resilience capabilities and ask the right questions. At the end of this paper, we present a series of questions that will help you in assessing your organization.

Increasing dependence on connectivity in our world today makes data protection a critical issue for all. The key challenge is interdependence even in a world with different governmental restrictions; no single organization can resolve data protection and privacy issues alone. A collaborative, multi-stakeholder approach must be taken, even if this requires competitors in a given industry to partner in the effort to ensure a stable and safe environment.

> *“Cyber resilience is one of the top issues out there for governments and industry. There are no boundaries when it comes to cyber warfare. It crosses boundaries. There’s no geographic block here when it comes to this kind of an attack.”*
>
> Michael Roach, president and CEO of CGI, during an interview with Business News Network on March 13, 2013.

Data security risks in a hyperconnected world

Our world is increasingly connected through sophisticated networks, Internet commerce portals, mobile devices, tablets and other innovative tools that create opportunities for economic growth, innovation and convenience. As businesses, governments and individuals become more reliant on these connections, valued data assets are increasingly vulnerable and cybersecurity threats multiply.

Cybersecurity risks have a broad impact:

- Consumers are subject to personal data/identity theft, fraud and inferior counterfeit or pirated goods.
- Businesses risk losing intellectual property, corporate secrets, reputation, the value created by innovations, and revenue through espionage and breaches.
- The storage locations of data may be governed by different laws and regulations, creating access issues as well as increased risks.
- Increased data flows across global corporate networks make data protection complex and difficult to ensure.
- People who work offshore may copy client data to meet local government requirements or for marketing campaigns, exposing it to security threats.
- For a nation‟s broader economy, business and individual security losses impact GDP, reduce economic growth and innovation, and result in a smaller tax base.
- For governments, espionage and cyber attacks threaten national security and diplomatic relations.
- Critical infrastructures providing communications, transport, water, power, food and healthcare are becoming more attractive targets for attacks.

Recent publications estimate that the likely annual cost to the global economy from cyber crime is more than $400 billion. Cyber criminals are more sophisticated, focused and better funded than ever. And, crime follows monetization opportunities. There is an emerging correlation between the size of an organization and the type of data targeted.

Data of strategic significance, such as trade secrets and other intellectual property, is becoming more of a target within larger organizations.

On the other hand, the cost or risk of engaging in cyber crime is often very low relative to the payoff. Attribution and „chain of custody" issues make prosecution by law enforcement difficult. In some cases, even when criminals are prosecuted successfully, the penalties are not significant enough to be a deterrent. However, new European Union legislation imposes high penalties for cyber crime.

The major challenge for organizations today is determining how to embrace innovative technologies and trends such as „everything connected‟, cloud, mobile and social computing, while at the same time managing the inherent data risks and privacy laws that conducting business in cyberspace demands.

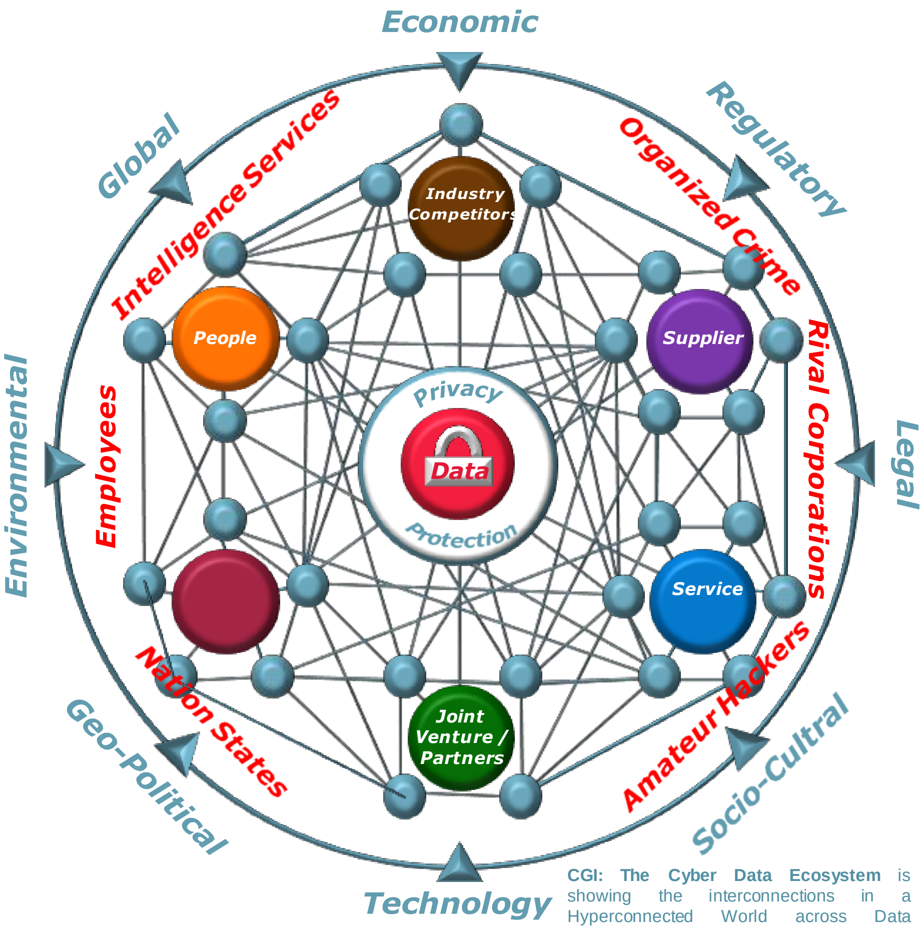
"Forrester predicts that NSA disclosures may reduce U.S. technology sales overseas by as much as $180bn, or 25% of IT services, by 2016."

"NSA Spying Seen Risking Billions in U.S. Technology Sales," *Bloomberg,* September 10, 2013.

The cyber data ecosystem

In today‟s business environment, disruptive technologies such as cloud computing, social computing and next-generation mobile computing, as well as the interconnections among corporate networks and the Internet are fundamentally changing how organizations use information technology (IT) for sharing data and conducting commerce online. This wave of technology innovation has created unparalleled levels of access and connectivity across people, data, systems and assets worldwide, transforming today‟s cyber data ecosystem.

In the cybersecurity arena, the increasing sophistication, frequency and scale of cybercrime as a result of this open and network-oriented society, coupled with the recent explosion in the use of „edge‟ devices and cloud-based applications, as well as increasing regulation, has created an urgent need for organizations to rapidly advance their data security countermeasures and re-think traditional approaches. On a more global level, due to the compelling and pressing nature of the issues involved, many countries have elevated cybersecurity to a top-tier priority within their national security strategies.



CGI: The Cyber Data Ecosystem is showing the interconnections in a Hyperconnected World across Data Relationships and the Interacting Factors.

To stay ahead of escalating risks while at the same time manage costs, business leaders need to consider a broader data risk management strategy that addresses the numerous disruptive trends taking place today. By understanding the complexity of the cyber data ecosystem and the major domains it represents, enterprises can implement their cyber strategies and develop specific plans tailored for each domain and exposure area in a holistic manner.

"In the USA, before Snowden, the use of Internet services for email, etc., was presumed ethical and within most statements of standards of care by U.S. bars because government was presumed to be protecting the security and integrity of Internet communications."

"The Snowden Revelations‟ Impact on Legal Practice," Lon A. Berk, Hunton & Williams, *Law360*, August 14, 2013.

Key focus areas should include the following:

- **Data assets, risks and business criticality**

  Understanding the nature of your data assets, their vulnerability to threats and their value to the business is a key step in defining what level of protection is appropriate. This is an ongoing process that not only helps to ensure security but also the most optimal use of your limited resources.

- **Users (identity assurance, regardless of location or device type)**

  Ensuring key data is accessible only by authorized users is essential to protection and privacy. Organizations must develop strong mechanisms to grant, revoke and audit access rights based on specific user entitlements or attributes.

- **Data protection (sensitive data protection, no matter where it resides)**

  Given the highly distributed nature of data, organizations must adapt their security approach to include mechanisms for protecting data outside the traditional enterprise perimeter and, most likely, data that is in a constant state of motion across many jurisdictions.

- **Data privacy requirements (depending on national laws and regulations)**

  Privacy and cybersecurity must be more tightly aligned than ever in this highly connected world. Risk and privacy assessments and controls need to be unified and address data capture, protection and breaches or disclosures across many privacy regimes.

- **Infrastructure protection (securing the 'borderless' enterprise, including cloud computing and mobile connectivity)**

  Protection of core infrastructures is essential to the resiliency of key systems where access to and the integrity of data is critical. This need is amplified as operational technology and information technology are now tightly linked and subject to the same threats. This again requires a change from traditional security approaches.

- **Data governance and compliance**

  The average organization is likely subject to more than a dozen regulatory mandates with which they must comply. This is in addition to business specific cybersecurity best practices they choose to adopt. Redefining data governance will ensure enterprise clarity on the creation, movement, storage and destruction of data in a compliant and secure manner.

The challenge is far broader than simply addressing one issue such as securing data, networks, mobile devices or cloud computing environments. By ensuring a cyber resilience strategy that addresses all of these interrelated trends, business leaders can be confident of a holistic defense-in-depth approach.

For businesses and governments alike, getting the cyber resilience posture right across all key areas is vital for future growth, innovation and competitive advantage.

> *"U.S. technology providers MS, Google, Mozilla, Twitter, Yahoo are in a 'digital arms race' to plug vulnerability to outside surveillance, directly as a result of the 'Snowden effect,' including higher levels of encryption, e.g., Transport Layer Security (https prefix) and even stronger Perfect Forward Security."*
>
> *International New York Times,*
> December 6, 2013.

Data strategies in the cyber data ecosystem

No matter which strategy is adopted, data breaches will occur. It is nearly impossible to take advantage of our connectedness without facing threats and attacks.

Defensive technologies such as firewalls, passwords, encryption, physical barriers and authentication mechanisms are important to maintain but these alone have been ineffective in eliminating breaches or predicting where the next attack will occur.

Their value as stand-alone security measures will be of limited use in fighting increasingly sophisticated, innovative and well-funded cyber criminals who are trying to steal your data or to disrupt your processes.

A predictive approach to threat identification and mitigation

The emerging challenge is to find more predictive methods of identifying threats, mitigating their impact and managing an agile cybersecurity operation that will creatively, proactively and effectively ensure data protection. In tackling that challenge, it is important to recognize the following:

- It is not economical to protect every piece of data and every asset to the same extent.
- A balance between the right to privacy and the need to protect nations, enterprises and individuals from intrusions must be negotiated.
- Attribution and severe penalties for cybercrime must be more uniformly realized within multi-national communities.

The challenge is great and requires new ways to blend people, processes, technology and shared data to protect societies from emerging security threats.

Designs and plans for cyber resilience should be data driven and predictive, rather than reactive in nature. Shared intelligence among countries and organizations is critical.

Combining data sources to support predictive analytics

Most organizations collect data internally, representing one data source. Increasingly, organizations are combining their data with that of other trusted public and private sources, discovering that the predictive value of broader data analytics increases exponentially.

Analysis of larger data sets reveals correlations and patterns of current threats that a single source simply cannot. Additionally, it allows emerging threats and command/control mechanisms to be quickly identified so that each participating organization can adjust security measures to mitigate these threats and protect valuable assets.

This collaborative approach to sharing data has barriers to overcome:

1. It is human nature to hide vulnerabilities rather than reveal them. Demonstrating the specific value derived from sharing security data may help to garner participation.
2. Each nation has laws governing disclosure of data breaches, and those laws are inconsistent. For example, U.S. law requires organizations to disclose certain data breaches, but laws in many European countries do not require the same disclosures. What may be acceptable and expected

> *"Greater awareness of / focus on communications and cybersecurity by business and consumers - they're all at it in the EU, and some aren't even as transparent and as controlled as the NSA."*
>
> Christopher Wolf, Hogan Lovells, *Financial Times*, July 16, 2013.

disclosure in one country may not be so in another, creating another barrier to sharing data among countries.

3. A level of distrust may exist among those considering collaboration based on the fear that sharing data may expose trade secrets and vulnerabilities. Understanding the qualifications of collaborators will influence an entity‟s willingness to share data.
4. The balance of privacy and disclosure is difficult to navigate, and privacy rights may limit government surveillance to protect democratic processes.

Data sharing across geographies

Many countries have in place or have started to develop data protection and cybersecurity strategies to enhance their reputation for governing and securing cyberspace. A key force behind these strategies has been increased cooperation among businesses and governments to share threat information and risks. Additionally, many industry sectors have joined together to rehearse contingency plans or jointly tackle vulnerabilities.

Many national governments and large trading blocs, such as the European Union, are reviewing current data sharing agreements with other countries such as the U.S., with the aim of ensuring equality in terms of data protection. Similarly, many governments are advocating technical measures for restricting Internet traffic; this is often referred to as „clean pipes‟ and is a very sensitive and political topic.

The shaping of traffic and the analysis of „threat inducing traffic‟ within a particular geography supports a holistic security approach to protecting a global organization and its networks and systems from being compromised. However, for a number of multi-national companies, seeking ways of sourcing more local suppliers, the lack of global consistency greatly diminishes the value of this.

Many organizations and customers have experienced the exploitation of vulnerabilities within company networks and the theft of data like credit card information or the misuse by organizations holding large data sets like patient medical records or social media data. Often the exploitation had occurred through a third party into the more valuable parent organization.

The nature of the Internet makes it difficult to identify who is behind an attack. If the attacker is identified, law enforcement often has limited resources to direct towards prosecution of these acts, and laws often do not match penalties with the severity of crime.

In general, this responsibility extends to governments, law enforcement agencies, and societies as well. The missing links in the chain of responsibility often involve attribution of criminal activity to an individual or group and resulting prosecution/penalties for these crimes.

Trans-Atlantic information sharing among governmental security and law enforcement agencies provides opportunities for more robust threat intelligence, greater protection, and more collaboration in mitigating attacks. However, unlike an institution like Interpol the sharing mechanisms don‟t exit and for many Governments cyber-threat data is dealt with at very high level of classification making general information sharing next to impossible, even with trusted partners.

Even with these mechanisms in place, commercial organizations need to understand the business value of this amalgamation of threat data and the benefits that it can bring to them. For a large multi-national with its own cyber resources this is possible but for a medium-enterprise and smaller the value and relevancy has to be delivered in order for them to commit to the process.

> *“Belgian government postpones €15-20m g-cloud project, mainly because of security concerns arising from Snowden revelations.”*
>
> *DmEurope,* January 20, 2014.

Data privacy regulations in the cyber data ecosystem

Data privacy regulation, when looked at globally, forms a spectrum of maturity beginning with spotty industry or situation-specific laws all the way to omnibus frameworks. As you might expect, responsible corporations prefer to engage in business practices where the data privacy laws are clearly defined and transparent.

Geographical differences in privacy protection

Compared to international standards, the U.S. takes an almost laissez faire sector-based approach to privacy law, concentrating on a handful of specific areas of data management (e.g., medical records, credit reports, children, electronic surveillance, etc.) Even with its privacy laws, the U.S. leaves most areas of personal data processing largely unregulated.

By contrast, jurisdictions with omnibus data protection laws, such as the European Union and Canada, regulate all data related to identifiable people. Because foreign data laws are comprehensive, they reach even seemingly innocuous databases such as telephone books, restaurant reservation systems, and personal online blogs. And, these foreign data laws impact core aspects of business operations, such as invoicing, personnel records and customer records.

The difference between U.S. privacy regulation and omnibus data protection laws, in large part, relates to the jurisprudential gulf separating the U.S. from other countries. The First Amendment of the U.S. Constitution grants people in the U.S. an explicit right to discuss, print or post online most information available about others, without any express exception for speech that might intrude on someone‟s claimed privacy. The First Amendment elevates free speech interests above privacy concerns. As such, the U.S. Constitution actually protects would-be privacy violators more explicitly than potential victims of privacy breaches.

Europe, Canada, and other jurisdictions with constitutional privacy protection and comprehensive data protection laws come at this issue from an entirely different perspective. Rather than putting privacy interests on a scale counterbalanced by free speech rights, these countries analogize privacy rights with intellectual property rights. If government is going to let corporations keep competitors from exploiting brand names and trademarks, the law certainly should allow a citizen to keep others from trafficking his credit history, sex life and other personal information.

European Union privacy law

Corporations either based in the European Union or wishing to conduct business there must comply with the standards of the EU‟s strict 1995 Data Protection Directive whenever data is transferred outside its borders. In 2012, the EU proposed a data protection reform package, stating that the current rules on data protection needed to be modernized in light of rapid technological developments and globalization. This reform package is expected to be accepted by the European parliament at the end of 2014.

Under EU law, personal data can be gathered legally only for a legitimate purpose and under strict conditions. Further, persons or organizations that collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners, which are guaranteed by EU law.

> *“Review of EU Data Retention Directive, 2006/24/EC, already challenged legally in opinion by Advocate General Villalon in Digital Rights Ireland case, thought to be heavily influenced by Snowden revelations”*
>
> “EU to force big changes on the big-data landscape: The EU is determined to overhaul the rules over who holds your personal data,” *The Irish Times*, December 19, 2013.

> *“Europe must stand united on this matter which is at the heart of European values, which concerns directly the fundamental rights of EU citizens.”*
>
> “EU justice commissioner Viviane Reding backs strict data privacy,”

Every day within the EU, businesses, public authorities and individuals transfer vast amounts of personal data across borders. Conflicting data protection rules in different countries would disrupt international exchanges. Individuals might also be unwilling to transfer personal data abroad if they were uncertain about the level of protection in other countries.

Common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. You have the right to complain and obtain redress if your data is misused anywhere within the EU. Be aware that the EU data directive creates its own terminology, which is essential to master before discussing any EU privacy law issues.

An important aspect of the directive for businesses based outside of Europe, such as in the U.S., is the directive‟s extraterritorial reach. Because it would otherwise be easy to circumvent the directive by transmitting regulated data outside of Europe for processing offshore, the directive specifically prohibits sending personal data to any country without a „level of [data] protection‟ considered „adequate‟ by EU standards.

Many U.S.-based companies have been surprised to learn that EU data laws reach even information about company customers and employees transmitted to U.S. headquarters. A typical U.S. response is that the Europeans are overreaching when they impose their data protection rules on intra-company data housed at U.S. headquarters or on a U.S.-based server.

But, from a European standpoint, these data transfers, even though intra-company, nevertheless transmit personal data about European data subjects outside Europe‟s jurisdictional reach. To a European who takes comfort in the EU‟s tough data protections, transfers of personal data outside Europe, even intra-company transfers, raise a real risk that personal data offshore becomes susceptible to abuse.

Corporations are concerned that placing data within the borders of a state with high levels of governmental surveillance could put their customers and intellectual property at risk. While China and Singapore passed in 2012 a significant number of new data privacy laws, both have long histories of unregulated governmental surveillance practices, as does the U.S. as demonstrated by the Snowden case.

Corporations working within the borders of Mexico also worry about a 2012 Mexican law that gives the government unrestricted access to mobile geo-location data provided by carriers. Within the EU, Sweden passed a new 2012 data retention law in line with the EU Data Retention Directive, giving the Swedish government broad surveillance capabilities.

Because information is a powerful business asset, modern businesses need to have the know-how to operate in this increasingly hyperconnected global economy.

Executive responsibilities in the cyber data ecosystem

Following are 10 critical questions every CEO, executive and senior manager should ask in assessing their organization‟s cyber resilience in today‟s hyperconnected world.

"Growth of Canadian data centre business as U.S. and foreign companies relocate data from US to Canada. Canada viewed as safe haven for cloud computing; U.S. stands to lose billions in business as companies look north to store data"

The Toronto Star, January 9, 2014.

1. Who is accountable for protecting our critical data?

In most companies, there is shared accountability between business managers and corporate information security officers (CISO) in securing critical data across the organization. These officers ensure that security is a consideration at the outset of new business initiatives and provide security expertise to business units.

2. Do we know what and where our most important data assets are?

Cyber data assets that are most critical to the accomplishment of an organization‟s mission need to be protected from data security risks and, therefore, it is important to know what your most valuable data assets are and where they are located. In a large and complex enterprise, it is difficult to assess how problems with a portion of critical cyber data assets may affect the broader operational mission.

Allowing data to move beyond your company‟s physical control by outsourcing data storage, sharing inventory information with suppliers/customers or running software on a cloud computing provider‟s platform all pose new challenges related to data location, ownership, privacy and protection laws and regulations. Investing in a good inventory/asset management system for your critical data assets is key to maintaining business continuity.

3. Are we meeting expectations regarding data privacy for our customers and our employees?

Financial services organizations and healthcare providers are required by law in the U.S. to protect personal information about customers and patients. Some countries require all businesses to do this, and most countries require businesses to notify customers if their personal information is compromised. Organizations also need to uphold promises they make in privacy policies.

But organizations have an opportunity to go beyond compliance and gain consumers‟ trust amid growing concern about the amount of electronic data that companies collect, analyze and share. For example, smart grid operators can use privacy protection to gain credibility among customers and encourage them to participate. Online advertisers that target ads to people based on products they view could also win their confidence by making it easier for people to opt out.

4. How can we ensure that we comply with regulatory requirements and industry standards in the most transparent, cost-effective and efficient manner?

Companies such as highly regulated financial services organizations face overlapping requirements. Costs can be reduced by mapping these requirements and conducting tests to demonstrate transparency and compliance with multiple regulations and standards.

As data flows between countries with disparate data protection laws, organizations need to ensure the safety of their customer and employee data through regulatory compliance and due diligence.

5. HOW DO WE TAKE ADVANTAGE OF OUTSOURCING & CLOUD COMPUTING AND STILL PROTECT OUR DATA ASSETS?

As they should do with all business partners, companies need to assess the ability of outsourcing or cloud providers to protect the confidentiality, availability and integrity of their data, as well as respect privacy laws and ensure transparency. Companies need to understand the risks related to how the outsourcer or cloud provider handles data from multiple clients or how it manages the third parties it uses. In contracts, they need to spell out requirements, including transparency, and how providers will mitigate the risks and handle data when the contract ends. Certification or third-party audits can be required to ensure that providers do what they promise. A cloud model also requires changes in how companies manage user data, log activity and identify and investigate events.

> *"Decision by German data protection authority July 24, 2013: no new authorisations for data transfers to non-EU states, pending reassessment of EU data protection arrangements for sharing data with governmental and private entities in third countries.*
>
> "The aftermath of the PRISM program and its wider impact," May and Carton, *E-Commerce Law & Policy*; August 2013.

6. HOW TO DEAL WITH DATA RISKS OF MOBILE DEVICES / BYOD (BRING YOUR OWN DEVICE) AND SOCIAL MEDIA?

While mobility boosts enterprise employee efficiency by delivering „anywhere access‟ to business data and systems, it obliterates what's left of the increasingly ineffective corporate network perimeter. Many security managers have already discovered the disconcerting implications; less control than ever over enterprise data access from a myriad of consumer devices, including a groundswell of bring your own devices (BYODs) and more difficulty in determining which devices are accessing which systems and data.

To ensure safe, effective use of BYOD in the enterprise, IT and security teams should work in partnership to assess emerging automatic tools that display the vulnerabilities in app code and provide a score for how well the apps can be trusted. Moreover, traffic from each device (and app) must be monitored to watch for things that it shouldn't be doing. These types of controls support less arbitrary permit/deny decisions each time a user carries in a new type of device. An organization can address many BYOD privacy and compliance concerns by focusing on secure business assets.

7. HOW DO WE ENSURE THAT ALL OUR EMPLOYEES ALWAYS VIEW SECURITY AS THEIR RESPONSIBILITY?

People are the key to security in a world where valuable corporate data is increasingly moving beyond a company‟s physical control. Employees who aren‟t trained to think about security can disclose sensitive data on social networks or click on sites that hackers use to infiltrate corporate networks.

Vigilant companies embrace social media and step up training. For example, CGI conducts security awareness training and has mandatory security compliance courses, with the view that „people are the new perimeter‟.

8. HOW DO WE PROTECT OUR OWN DATA AND THE DATA OF OUR CUSTOMERS?

Data protection should be considered at the onset of new business initiatives as a way to mitigate risk. CEOs and executive boards help articulate these objectives as they pursue growth. Data protection can‟t be an afterthought. In the power industry, for example, utilities need to incorporate data protection and security in the design of smart grids and with suppliers to protect all of the new points in networks where intrusions and data breaches can occur.

Based on the localization of your data, it‟s important to have a data protection strategy in place that covers the different geographic locations, as well as the corresponding data protection measures and controls in line with the privacy and data protection laws and regulations.

It is a good idea to periodically review your overall data protection and security strategy for your own data, as well as for your customers. Weigh risks against business needs, set company-wide priorities and use resources to protect data that, if lost, would cause the most damage. That can change over time as the business evolves.

9. Are we pro-actively looking for signs of systems and data breaches?

Hackers were once motivated largely by ego, but now they target valuable data that can be sold or used to steal money. Cases of state-sponsored espionage known as advanced persistent threats also target companies‟ intellectual property. Hackers‟ techniques have become more sophisticated, and they can hide evidence of attacks, remaining undetected for months or even years.

An important technique for proactively identifying system and data breaches is to strictly monitor outbound network traffic. Most advanced persistent threat malware, when infiltrated, is trying to contact the remote control center. This uncontrolled outbound network traffic could be an indicator of a compromise.

10. What is our plan for responding to a security breach?

Cyber threats are more rampant than ever before. A cyber attack can impact the performance of an enterprise or compromise sensitive data within minutes. To avoid this, governments, critical infrastructures and commercial organizations must implement preventive measures and develop a plan that enables rapid response and recovery through collaboration with customers and service providers.

Implementing a Cyber Security Management Framework, like CGI‟s CSMF ensures that recovery plan(s) are put in place for critical cyber assets and that these plans follow established business continuity and disaster recovery techniques and practices.

An effective plan can mean the difference between a quick recovery and a serious blow to your company‟s reputation.

Summary

Most organizations today maintain a perimeter-centric defense strategy (i.e., fire walls, etc.) for protecting their most valuable data assets. However, we are faced with a new reality. You can build numerous walls and fortifications for your organization but cyber threats will continuously evolve, and they have. Hackers have found new ways of getting around your wall or going through it.

Data security breaches are everywhere in both the public and private sector. Attacks can come from either outside or inside your organization by hackers, terrorists, foreign nations, criminal groups or your data owners, system administrators, among others.

A defense-in-depth cybersecurity strategy—combined with encrypting the data itself, implementing higher levels of data, identity and access assurance, and focusing on the highest risk-profile environment—can deal with most of the current threats.

However, you need to realize that, in real-time industrial and process control environments, encryption is not always an option due to the latency of encryption and decryption. That‟s why a defense-in-depth strategy is still important.

If cyber resilience is a potential risk to growth and competitiveness, it is also an enabler. Countries and organizations that invest in and develop data protection and cyber capabilities to instill trust in customers, citizens and investors will have a competitive edge in this digital era.

> *“10% of non-US resident organisations had cancelled a project with US-based cloud computing providers, 56% said that they would be less likely to use a US-based cloud computing service, 36% of US resident businesses said that the NSA leaks made it more difficult for them to do business outside the USA.”*
>
> “Survey Results: Government Access to Information,” Cloud Security Alliance, July 2013.

About CGI

A CYBERSECURITY PARTNER YOU CAN TRUST

At CGI, security is part of everything we do. For more than 35 years, we have helped clients manage complex security needs from audit and compliance requirements to policy and architecture development, with a business-focused approach. We work with leading corporations and government in the U.S and Canada, as well as across Europe. As a result, we understand security from all angles—technology, business and legal—and have a 360 degree view of global and local threats in both the public and private sectors.

We help our clients to protect their business by assessing and analyzing potential cyber risks, continuously monitoring for threats in real-time and putting in place the necessary defenses. Our end-to-end information security offerings include consulting, security engineering and managed security services. We cover governance, risk and compliance, and data risk management, as well as industrial control systems/critical infrastructure protection. We also provide identity and access management solutions, including biometrics, as well as cloud security and mobile security expertise.

We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies. We are one of the few providers worldwide with three accredited security certification facilities—located in Canada, the U.S. and the UK—including our world-class CGI Federal Cyber Innovation Lab. Our ten Security Operations Centers continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure, handling more than 70 million cyber events a day.

Founded in 1976, CGI is a global IT and business process services provider delivering business consulting, systems integration, cyber security and outsourcing services. With 68,000 professionals operating in 400 offices in 40 countries, CGI fosters local accountability for client success while bringing global delivery capabilities to clients‟ front doors. CGI applies a disciplined and creative approach to achieve an industry-leading track record of on-time, on-budget projects and to help clients leverage current investments while adopting new technology and business strategies.

> *"Non-U.S. based technology, telecommunications, hosting and cloud providers will structure their groups geographically – having separate companies in different regions."*
>
> "CloudSigma, Swiss cloud operator, already reported as having done so: Snowden saga reviews gaps in protection of European data," *The Financial Times*, July 29, 2013.