Closing the **Cybersecurity** Risk Gap

CGI

Experience the commitment®

Introduction

As a result of the cloud, bring your own device (BYOD) policies, mobile computing and the Internet of Things, we are now living in a hyperconnected world. Where people once accessed their bank accounts once or twice a week from one digital source, an ATM, they now access their accounts 4-5 times a day through multiple digital channels. More and more companies offer and sell their products and services online to meet increasing customer demands, and even household appliances are equipped with Wi-Fi chips.

All of these developments make consumers and organizations more vulnerable to cyber attacks. Hackers can even target refrigerators or televisions to get access to data and systems. Cybersecurity developments are moving so fast that the risks will only increase in the coming years. A key reason is that cyber criminals historically were isolated; smart individuals acting alone trying to hack a system just to see if they could. Now, they are part of organized crime and nation states with sophisticated teams and global scale seeking to steal and destroy.

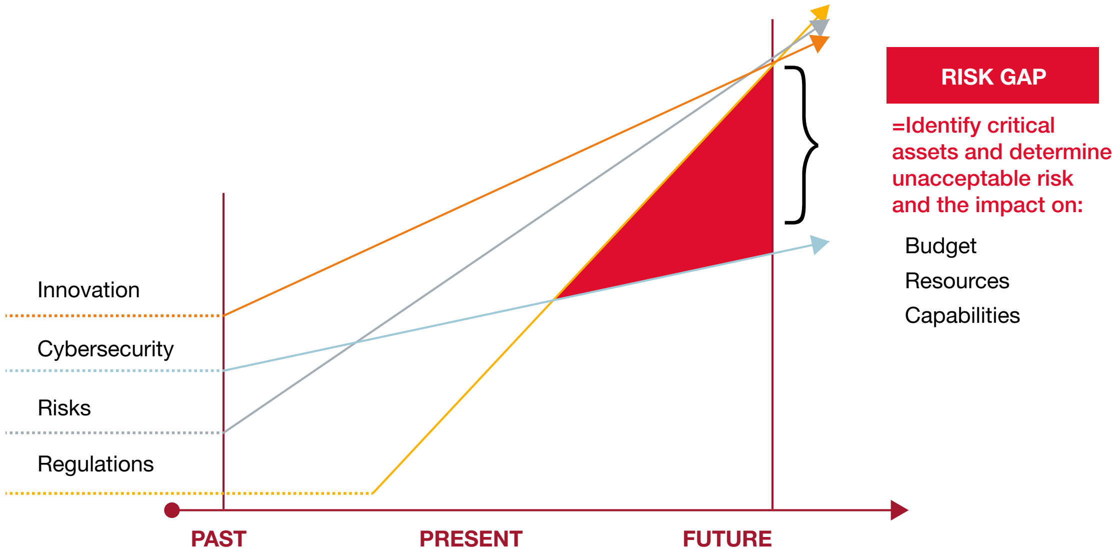
While regulation has increased to try and keep pace with growing threats, it is increasingly difficult and costly for organizations to comply with new rules. In the Netherlands, the new General Data Breach Notification law took effect in January 2016 aiming to increase the responsibility of those who keep or send citizen data, adding new levels of compliance for Dutch organizations.

This white paper investigates the gap between rapidly rising innovation, cyber threats and regulations as well as examines efforts to develop robust protection programs. It is informed by CGI's 2015 Voice of Our Clients program, which includes face-to-face interviews with client executives to get a pulse on industry trends and their business and IT priorities. In 2015, CGI interviewed 965 executives representing business and IT management across 10 industries and spread over 17 countries. In the Netherlands, 66 executives participated in the program. Comparisons are drawn between Dutch participants and those from other regions. Several recommendations have been made for Dutch organizations regarding priorities for addressing the security challenges of today's hyperconnected world.

The growing cyber risk gap

Three key factors—rapidly evolving innovations, risks and regulations—are combining to stretch traditional security models to their limits of efficiency and effectiveness, resulting in a large and growing cybersecurity risk gap. The urgency to close the gap is even greater when considering it.

The cybersecurity risk gap



=Identify critical assets and determine unacceptable risk and the impact on:

Budget

Resources

Capabilities

"All of the current metrics that measure the rate of threat increase, the extent of breaches and the business impact suggest that the potential of a breach occurring in any organization is highly likely, and may be inevitable," states research agency Pierre Audoin Consultants (PAC) in their white paper commissioned by CGI. The paper also recommends that organizations spend at least one-third of their cybersecurity budget on detection and response.

A boardroom topic

Cybersecurity is now a board-level concern. Our client interviews indicate that privacy and data protection are key focus areas at the C-level. Being prepared for the inevitable breach and closing the gap between current cybersecurity programs and rapidly evolving threats require having a very solid and thorough security policy for dealing with cyber risks. The policies must be supported by the boardroom to have the credibility and validation to ensure adoption throughout the organization. Increasingly, boards are focused on ensuring that executive management understands the business and IT risk and that they are well prepared.

The Netherlands perspective

While cyber risks are global and affect organizations across regions, we have included several comparisons between the interview responses of our clients in the Netherlands and those from other geographic regions.

Cybersecurity as a top IT and business trend

Across all industries and regions, this previous IT-centric issue is now a top business concern for our clients. In fact, client interview participants from the Netherlands ranked cybersecurity threats as the second-highest trend after cost/budget pressures, as compared to all participants globally ranking cyber threats as the fifth-highest trend. The difference may be the result of the Netherlands being such a highly digitalized society, making it more vulnerable to cyber attacks, as well as high levels of cyber awareness created by Dutch government campaigns and media coverage of high-profile attacks where Dutch companies and consumers were directly impacted. Research shows companies are aware of the high risk of cybersecurity; in the Netherlands even more so than in other parts of the world.

Top trends

Global	The Netherlands
1. Increased customer/citizen demands	1. Cost/budget pressures
2. Accelerate digital transformation	2. Cybersecurity threats
3. Deliver regulatory compliance	3. Increased customer/citizen demands
4. Address cost/budget pressures	4. Digital transformation
5. Protect through cybersecurity	5. Regulatory compliance

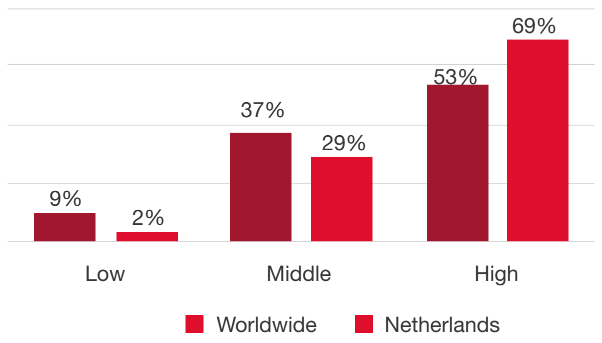
Source: 2015 CGI Voice of Our Clients program

Confidence in current cyber protection

When asked how confident they were in their current cyber protection measures, 53% of all interview participants indicated they were confident or very confident. The Netherlands participants had a significantly higher percentage (69%) indicating confidence or high confidence.

[1] 'Is a cyber breach inevitable? Cyber Security Challenges in The Netherlands,' by Pierre Audoin Consultants (PAC) Ltd, commissioned by CGI (2015): http://www.cginederland.nl/whitepaper/cyber-security-challenges-in-the-netherlands

Executives’ confidence in their organization’s cybersecurity protection



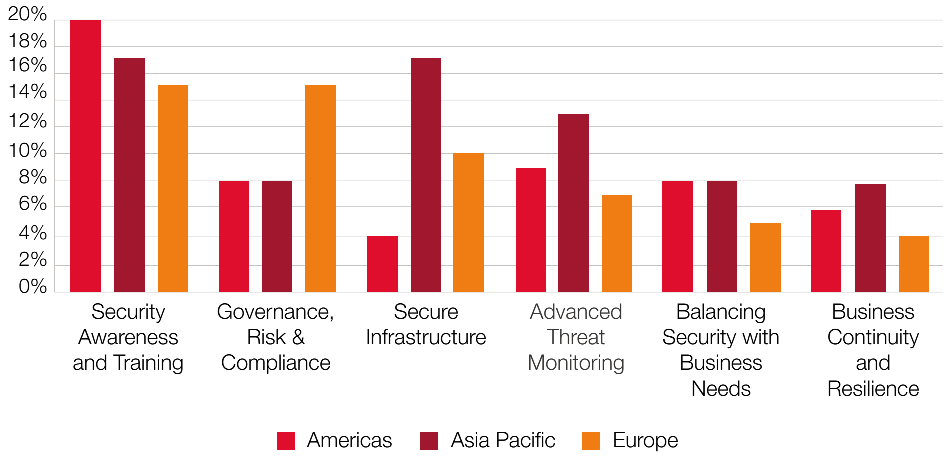
Source: 2015 CGI Voice of Our Clients program

The higher confidence levels may reflect a past and current emphasis by the Dutch government to reduce cybersecurity risk, including regulatory and legislative changes, by putting greater controls in place. Another factor may be the high levels of cyber maturity in the Netherlands evidenced by the Information Sharing and Analysis Centres (ISACs) established in critical infrastructure industries such as utilities, telecom and financial services.

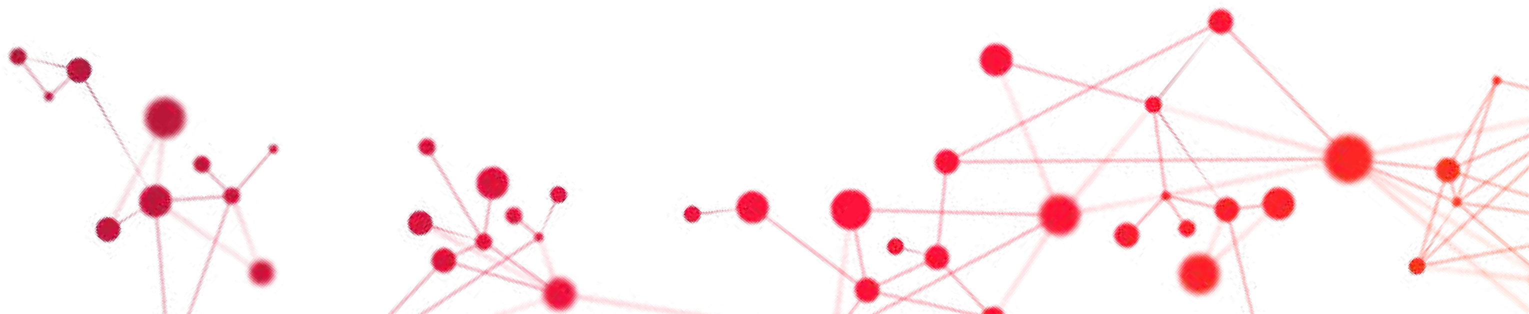
Top cybersecurity priorities

Across all regions, raising awareness of cybersecurity and governance, risk and compliance are key priorities. The variances shown among North America, Europe and Asia Pacific participants may reflect different regional awareness levels and legislative environments.

Top cyber priorities by region



Source: 2015 CGI Voice of Our Clients program



The Netherlands

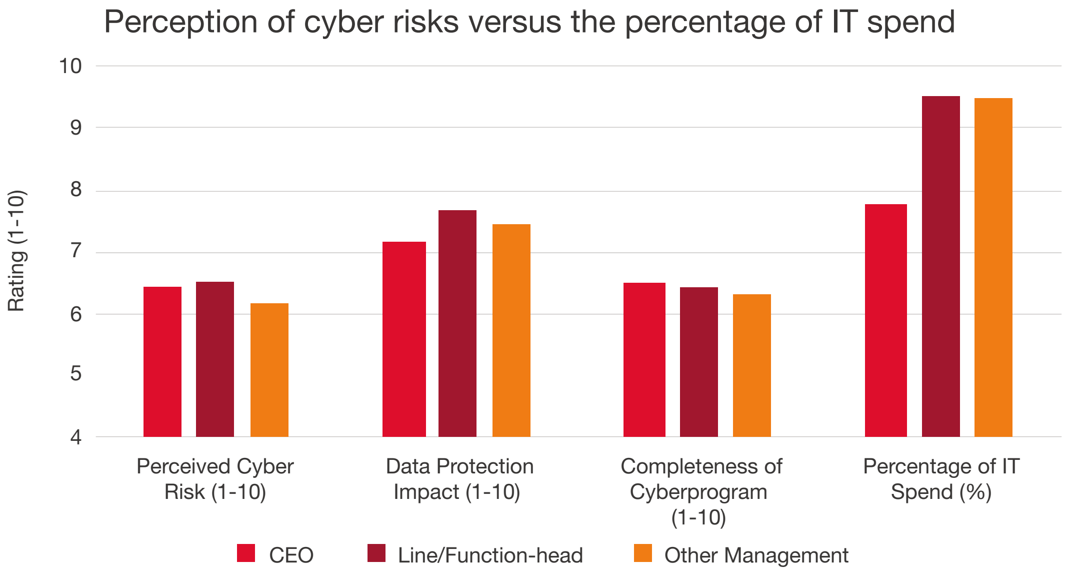
While the Netherlands participants indicated having essentially similar priorities as other regions, there was a higher focus on privacy/data protection as well as threats and risks assessments. It could be the result of the country's cyber maturity, strict legislation and increased awareness around the new law on General Data Breach Notification.

Progress made but more is needed on fundamentals

We also asked our clients questions related to their progress in developing a mature cybersecurity program. The programs should cover all of the fundamental bases, such as executive-line management alignment, critical asset identification, robust incident response plan, understanding of financial impacts and assessing strategic risk. Likely due to the rapid change occurring in the cybersecurity environment, the responses indicate that actions taken have not progressed to keep pace.

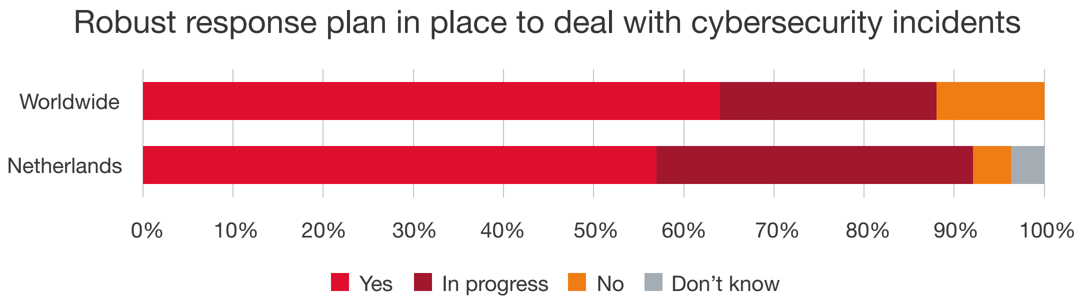
Board-line management alignment

Although cybersecurity is now a board-level concern, our client responses indicated a potential difference in the perception of cyber risks and the adequacy of security measures between executive management and line management. Responses from participants at the line management level indicated higher perceptions of cybersecurity as a risk than did executive management participants. It could be due to the fact that they tend to hear more about issues around cybersecurity and are closer to its programs and activities.



Incident response plans

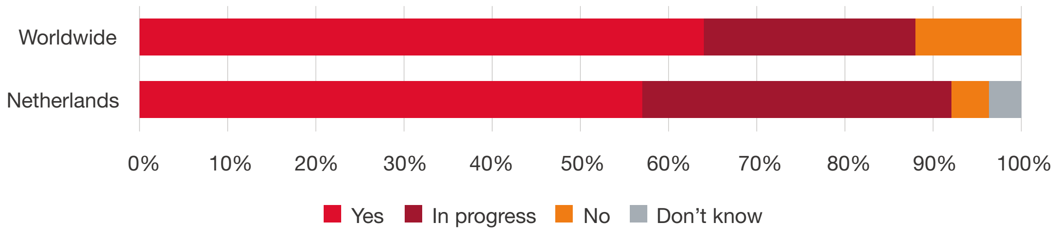
While 67% of all participants said they have a robust incident response plan in place, among participants from the Netherlands, the percentage was 55%. A robust incident response plan must include regular reviews and continuous testing to ensure the plan is comprehensive and protects all aspects of the organization. Ensuring that employees are trained in security policy and are aware of current email and phishing schemes will help employees understand that they are the front line defense in any organization.



Asset inventories

When it comes to documenting assets that are attractive to cyber criminals, 67% of all CGI client interview participants indicated they have done so. Among the Netherlands participants, 57% responded they have done the documentation. Identifying these assets is a fundamental part of any cyber program.

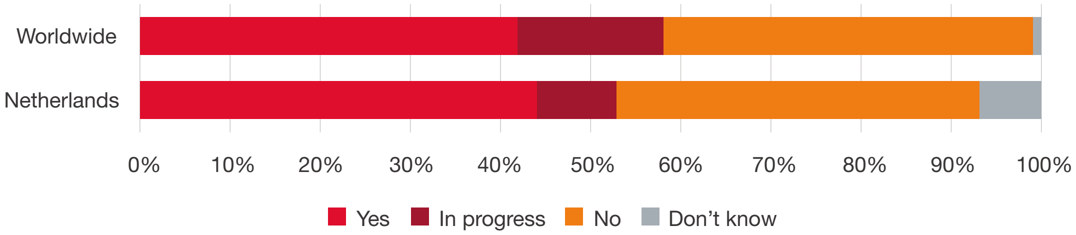
Identified assets that are attractive to potential cyber crime



Cyber insurance

Cyber insurance is gaining popularity in both the Netherlands and globally. According to the Association of Insurers, insurance companies will develop cyber insurance at a fast pace in the coming years. Among participants in our client interviews, 42% indicated that they conduct an annual evaluation of the use and need for cyber insurance. Among the Netherlands participants, the rate was just slightly higher (44%). The decision to have cyber insurance strongly depends upon the coverages and premiums available, which differ significantly from insurer to insurer in this emerging market. At the heart of the variation are differences among insurers in their ability to accurately assess policyholders’ cyber risks and to respond appropriately to claims.

Annual evaluation of cyber insurance protection



Industry views on cyber risk

The client organizations included in our interview program represent a variety of industries, including financial services, healthcare, manufacturing, transport, utilities, communications and government. While participants indicated similar trends across industries, investment priorities did vary by industry. Logically, investments were higher in industries perceiving a high risk of attack or having experienced direct and sophisticated attacks. This was true for financial services, oil and gas, utilities and government sectors.

Within government, growing security risks caused by digitalization, multi-channel services and outside threats of online services require more intergovernmental agreements and tools for better cooperation and protection of government services. Naturally, cybersecurity is a top priority within the defense sector. In manufacturing, more than 50% of interview participants said they considered cybersecurity as a significant risk. Among healthcare and life sciences participants, cybersecurity was not yet ranked at the top of their IT agenda, but it has climbed as a trend since our 2014 interviews.

A sampling of representative client comments on key cybersecurity priorities:

Industry	Comment
Financial Services	"Awareness and responsibility must be fostered throughout our organization."
Government	"Cyber criminals keep getting smarter, and they work 24/7." "How do we create secure working environments that are realistic and workable?" "Our focus is on security initiatives to protect our most vital information resources."
Healthcare	"We need a more holistic view of what happens in our current systems."
Utilities	"How do we educate employees to protect them from being misled?" "Integrating IT security plans with physical security plans is critical."

Conclusions and recommendations

9

Conclusions

- Cybersecurity is now a board-level concern, with most organizations perceiving the risks as high. CGI's client interviews indicate that privacy and data protection are focus areas at the C-level, while responses from line management show greater focus on security awareness and training. Board-level responses present a more optimistic view of cybersecurity risks to their organizations than do line manager responses. A lower sense of cybersecurity risk in the boardroom is an extremely important issue to address, as C-level commitment is essential for organizations to take the necessary steps to protect the business and operate with confidence.
- According to CGI's worldwide annual client interviews, most organizations feel confident in their current level of protection against cyber crimes. Confidence is even higher in the Netherlands thanks to the high level of cyber maturity and cybersecurity campaigns by the government amongst others. Awareness of cybersecurity has also increased due to more media attention especially around such topics as high-profile attacks. Organizations are also confident in their security plans; however, when examining their cyber programs more closely, this confidence is not always justified by their actions.
- Even though cyber breaches are inevitable and while organizations across all countries and industries are confident in their levels of protections and security plans, many organizations still have not completed a robust response plan to deal with cybersecurity incidents. Also, there are still several organizations which have not completed the identification of organizational assets attractive to cyber criminals.
- Surprisingly, almost half of the organizations do not conduct annual evaluations of their security programs, which suggests that many organizations have a more positive view in terms of the levels of preparedness and security plans than their actual actions and 'ready-to-act' plans indicate.
- Investment in cybersecurity is generally prioritized by industries that perceive a high risk of attack or have experienced direct and sophisticated attacks such as the oil & gas industry, financial services, utilities and governments. However, with the growing awareness and risks in regards to cybersecurity, it is perhaps only a matter of time before organizations across all industries see the need to prioritize cybersecurity and their investments.
- Organizations need to be aware that the level of cyber threats has increased and cyber criminals are becoming more professional. They were once merely smart individuals trying to hack a system just to see if they could. Now, it is often organized crime with sophisticated teams on a global scale trying to steal and bring down companies, which requires a more professional approach and response to the current cybersecurity challenges organizations are facing.

Recommendations

10

When seeking to protect themselves from cyber attacks, many organizations respond by procuring technology, but a mature response strategy must cover the fundamentals. It is important for organizations to step up their cybersecurity efforts in a number of critical areas. CGI has identified four common areas for improvement to help organizations bring their cybersecurity efforts in line so that they can close the cyber risk gap.

1. **Align risk perceptions at all levels.** When the perceptions of executive management differ from the rest of the organization with regard to cyber risks and the adequacy of security measures, this can lead to a mismatch between the perceived risks and the actual measures taken. As a consequence, executive levels may be exposed because they are accountable for the business impact of security incidents. Organizations therefore need to align risk assessment and security measures at all levels. This requires that management boards are not only aware of cyber risks, but are also periodically informed of the security position taken by the organization.

2. **Identify critical assets at risk.** Identifying the assets in an organization is a fundamental part of the delivery of any cyber program. Organizations too often lack a complete identification of critical assets, making the development of an appropriate cybersecurity program very complicated. They should therefore identify the critical assets and assess the extent to which these assets are at risk of a cyber attack. Based on the inventory, organizations can build an appropriate and accurate cybersecurity program. Both the critical assets and protective measures need to be evaluated periodically.

3. **Develop a cyber incident response plan.** Despite all preventive measures, history shows us that cyber incidents will happen so the key is to have a response plan in place. Organizations need to monitor the cybersecurity threats on a continuous level (24/7), to develop robust incident response plans and the accompanying capabilities in the organisation to carry out the response. Only then will they be able to detect and respond timely and adequately in the event of cyber incident. Given that it can be difficult to develop cybersecurity capabilities internally, outsourcing security monitoring and responses are a viable option.

4. **Assess the potential financial impact of incidents and consider cyber insurance.** Even with proper insight into cyber risks, a complete identification of critical assets and adequate monitoring and response capabilities, there is still a risk cyber incidents can affect organizations. Incidents can have financial repercussions on organizations if crucial business processes are interrupted or when partners or customers are impacted. New legislation, such as data breach notification laws, increases the financial risk. Cyber insurance, which has matured quickly in the past years, can help to cover the possible financial impact of cyber incidents. Organizations must assess the potential financial impact of cyber incidents and consider cyber insurance to cover the risk. To better assess cyber risks and obtain cyber insurance which comes with a reasonable premium and the required coverage, it is essential to have a thorough inventory of the assets that are attractive to cyber crime. Demonstrating that well-prepared response plans are in place is also indispensable when applying for cyber insurance.

CGI advises its clients to start with a strategic risk review of their organization's assets to gain a detailed understanding of the current state, including what the loss of confidentiality, integrity or availability means to the enterprise in objective (i.e., money) and subjective (i.e., reputation) terms. The next step involves developing a security roadmap, which may include a technology purchase, or an outsourcing or partnering strategy.

Conclusion

Many participants in CGI's 2015 client interviews felt confident in their current level of protection against cyber crimes. Yet, since the level of cyber threats has increased and cyber criminals are becoming more professional, it will require more professional preparation and response. To keep ahead of the curve, it is important to be proactive in analyzing and assessing the systems to prepare for the latest threats since a breach is virtually inevitable.

While a solid cybersecurity policy needs to address how to react when a company is actually facing a security incident, it is recommended that it start with a complete inventory of organizational assets that are attractive targets for cyber criminals. Strategic risk assessments, periodic evaluations of the policy and evaluating cyber insurance also need to be considered.

About CGI

Founded in 1976, CGI is one of the largest IT and business process services providers in the world. We combine innovative services and solutions with a disciplined delivery approach that has resulted in an industry-leading track record of delivering 95% of projects on time and within budget. Our global reach, combined with our proximity model of serving clients from 400 locations worldwide, provides the scale and immediacy required to rapidly respond to client needs. Our business consulting, systems integration and managed services help clients leverage current investments while adopting technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our client satisfaction score consistently measures 9 out of 10.

Cybersecurity is part of everything we do and for over 35 years, our government and commercial clients have regarded us as their cybersecurity expert of choice. Cyber attacks are becoming more sophisticated and can lead to financial loss, reputational damage, theft of business-critical information or regulatory fines. We have helped our clients build cybersecurity into their corporate strategy so they can conduct business in a digital age with confidence, openly and globally, driving competitive advantage, efficiency and growth.

For more information, please contact CGI at:

T: +31 (0)88 564 0000

E: cybersecurity.nl@cgi.com

www.cginederland.nl/cybersecurity