Deloitte.

From thoughts to action

The State of Cyber Security in the Dutch Caribbean

October 2016

Table of contents

“The threat is real. Banks are an obvious target for cyber criminals. But what about everyone else? Cyber criminals seek out easy targets, wherever they are. Think you’re not an obvious target? Think again.”

"As the world and the Dutch Caribbean become more interconnected, cyber security should be a key topic on the agenda of the Board and C-suite"

Mario Flores
Partner Risk Advisory

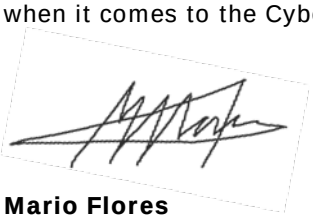
The actuality of Cyber Security

Last Friday one of the biggest Cyber Attacks took place in the US and Europe. The attackers struck in an unexpected way by turning ordinary devices into weapons. Hundreds of thousands of (home) devices, like webcams, DVRs and security camera's, were infected by malware and used to perform a massive distributed Denial of Service attack. This attack was targeted at a middleman, and through this way websites like Facebook and Netflix were victimized.

Incidents like this shows us the urgency of addressing the topic of Cyber Security. This particular example may have been outside of the Caribbean in an environment that seems more obvious for threat, but it would be naïve to assume that any industry in the Dutch Caribbean is not interesting for cyber criminals in one way or another.

Therefore, it is time to prepare. While companies in the Dutch Caribbean have been gaining insights for a while, it is now time to act. It is time to turn our thoughts into actions.

This Deloitte Cyber Security Study 2016 has investigated the readiness of the Dutch Caribbean in relation to Cyber Security. We would like to thank all the participants that have shared their thoughts and made this study possible. We aim to make this study a periodic event and follow the companies in the Dutch Caribbean in their path to make the Dutch Caribbean a more secure environment when it comes to the Cyber space.



Mario Flores
Partner Risk Advisory
Deloitte Dutch Caribbean

Introduction

With Cyber Security becoming a boardroom topic all over the world, Deloitte considered it time to investigate the maturity of Cyber Security in the Dutch Caribbean. This report contains the results of the Deloitte Cyber Security Study 2016: 'The State of Cyber Security in the Dutch Caribbean'.

Our world and society are becoming more and more digital at a very fast pace. The ways in which we are interconnected are increasingly complex. But new technology means new vulnerabilities and this comes with new attack vectors having an impact on organizations' security posture. Therefore, there is a need for active defences against existing and new cyber threats, current paradigms might not even be sufficient to combat all that's currently on our path. The question is: 'is your organization ready to defend itself?'

Purpose of the study
To obtain insight into the maturity of Cyber Security in the Dutch Caribbean Deloitte has executed the Deloitte Dutch Caribbean Cyber Security Study 2016. For the participants this was an opportunity to dwell on this strategic topic and discuss different topics that are trending in the field of cyber security.

Methodology
An extensive questionnaire touching on a wide range of Cyber Security topics was used during face-to-face interviews with relevant stakeholders from organizations in the Dutch Caribbean (mostly C-suite and IT management). These topics ranged from governance to security monitoring technologies to privacy. All these topics will be touched upon in the following chapters of this report.

Conclusion
Based on the differing conversations with the interviewees we can conclude that organizations in the Dutch Caribbean are very aware of the importance of the topic of Cyber Security. While some organizations have dedicated roles and in-depth policies and procedures for Cyber Security, other organizations are still struggling where to focus their efforts. Some topics that are receiving a lot of attention globally are not yet addressed that much in the Dutch Caribbean (e.g. privacy). Examples of these topics are cyber incident response (how to deal with breaches and/or other cyber security incidents?), mobile security, and privacy.

Industry differentiator
The intention for this study was to make a distinction between our findings within different industries. It has been decided, however, based on feedback received from the participants, the size of the market, and the size of certain industries that this would potentially be at the expense of the anonymity of the participants. Therefore this report does not contain industry specific findings.

Where relevant we compared the financial industry with other industries. Due to the number of participants in the financial industry this was possible without jeopardizing the anonymity of the participants.

Main findings:

- The responsibility for Cyber Security is often divided between multiple roles in organizations and isn't sufficiently addressed in the boardroom of organizations that participated in the study.
- IT budget expenditure on Cyber Security is expected to increase in the upcoming years, however, most of the budget is still spent on firewalls and other infrastructure security hard- and software.
- Security of mobile devices is a topic that organizations in the Dutch Caribbean are increasingly worried about.
- The human factor will always play a key role in Cyber Security. In the Dutch Caribbean more can be done to increase awareness about this important topic.
- Privacy will become a new concern with privacy regulations soon to be enforced.

Cyber Security in the boardroom

The increased strategic importance of Cyber Security demands an executive level approach to cyber risk management. Given this trend it is more relevant than ever that Cyber Security and accompanying risks make their way into the boardroom. Is it time for a Cyber Chair?

Various trend reports recognize the lack of boardroom attention to cyber risk management. There is still a gap in understanding the interconnectedness between information technology (IT) risk and enterprise risk management, especially given the rise of the Internet of Things (IoT) and other pivotal technological developments. Boards still are not undertaking key oversight activities related to cyber risks, such as reviewing budgets, security program assessments, and top-level policies; assigning designated roles and responsibilities for cyber security; How is the Dutch Caribbean dealing with this? Where should the responsibility for Cyber Security lie?

Why is it important to have an executive at the wheel for Cyber Security?

Cyber Security should be a top-of-mind issue for most boards, and the topic is becoming an enterprise wide issue rather than solely a concern for the IT department. Cyber-attacks can have heavily affect business operations as well as an organization's reputation, which could both have a huge financial impact. In these cases close involvement from the board is essential. Furthermore, the board plays an important role in understanding the risk associated with Cyber Security and ensuring that the right controls are in place for prevention, detection and response to cyber security incidents.

Roles and responsibilities in the Dutch Caribbean

There are multiple potential functions within an organization that could or should potentially be dealing with Cyber Security one way or another. Traditionally, Cyber Security was a responsibility assigned to the IT department, but we're not just dealing with IT anymore. Awareness on these developments with regards to cyber security have resulted in a shift of responsibilities, and executives are realizing it's their turn to act. Furthermore, organizations are increasingly setting up functions like a Chief Information Security Officer or an Information Risk Manager that (partly) deal with Cyber Security, in some cases even already reporting into the boardroom.

Figure 1 shows that more than 80 percent of the participating organizations in the study have an IT manager role, however, only less than 20 percent have a function like an

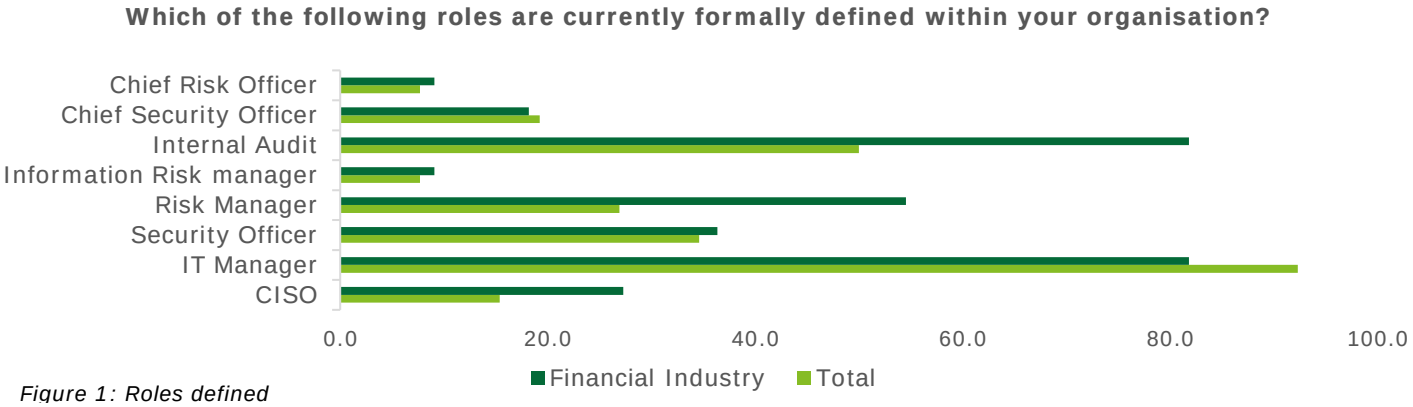


Figure 1: Roles defined

Information Risk Manager or a Chief Security Officer. The questionnaire results and additional conversations with participating organizations show that cyber security roles and responsibilities mostly reside in the IT department. As in other geographical regions, the Financial Services Industry is leading with necessary capability developments and this is also the case in the Dutch Caribbean. This translates into the presence of more executive level roles and responsibilities.

The roles as indicated in figure 1 are not in all cases involved in Cyber Security. In many cases Cyber Security still isn't a strategic agenda topic for roles outside of the IT department. Furthermore, the responsibility for Cyber Security is scattered between different functions that only have a part-time dedication to the topic. As can be seen from figure 2, most of the organizations have less than one Full Time Equivalent (FTE) dealing with Cyber Security. Analyst reports on global trends show that the size of the company has little influence on the number of security professionals, but between 70 and 80% of companies worldwide with less than 1,000 employees have between 1 and 5 security staff.

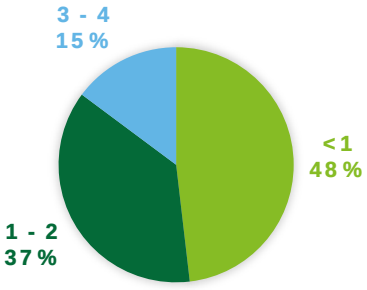


Figure 2: How many dedicated information security professionals does your organization have?

Boardroom topic

During the interviews we asked the participating organizations whether they considered Cyber Security to be a boardroom topic. As can be seen from figure 3 most of the organizations did consider Cyber Security to be a boardroom topic. Nevertheless we have determined that the actual focus on Cyber Security in the boardroom is still low. Some organizations also indicated that it should be a senior management topic.

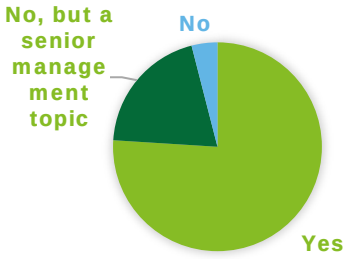


Figure 3: Do you consider Cyber Security to be a boardroom topic?

Barriers

Figure 4 shows what organizations in the Dutch Caribbean perceive to be the biggest barriers in becoming cyber secure. As an alarming number one budget is perceived as the most important inhibitor. In the chapter 'Cyber security budget' we will discuss this topic in more detail. Other barriers that have been mentioned are the increasing sophistication of the threats and emerging technologies, a lack of cyber security skills (both amongst personnel and in the marketplace), and clear roles and responsibilities within the organization.

"Explaining cyber security to the C-suite requires a totally different approach and language. The C-suite understands reputational risks, risks to their bottom-line, but not always the importance of investing in Cyber Security. It's time to reframe and speak a C-suite language, there's a lot at stake!"

Roy Jansen – Senior Manager Risk Advisory Deloitte Dutch Caribbean

Figure 4: Barriers in ensuring Cyber Security

Managing the human factor

Cyber Security is not merely an IT problem. Cyber attacks bypass sophisticated technical defence systems and take advantage of the human factor. Therefore, increasing awareness throughout the organization is key in becoming cyber secure.

Cyber security does not only involve having a secure IT infrastructure. When it comes to Cyber Security a large part of an organization's attack surface lies in the human factor. Common tactics, techniques and procedures (TTP's) that cyber criminals use to enter your perimeter is through social engineering. One of the most commonly known methods of social engineering is phishing, where a criminal attempts to obtain sensitive information by sending a seemingly trustworthy message via e-mail, MMS or WhatsApp or other communication channel, with a malicious link. In other cases incidents are caused by employee errors or omissions. While in the above mentioned events the negative consequences are unintentional, unfortunately the malicious activities from within the organization are too often also intentional. Therefore, managing the human factor is of critical importance.

Cyber Security Awareness in the Dutch Caribbean

Interviewees acknowledge the fact that the human factor is an important vulnerability to take into account. As can be seen in figure 5, from ten topics that have been rated on the probability of occurrence in the next 12 months, the top three topics highlighted as having a possible impact all involve the human factor. These threats are; employee abuse of IT systems and information, employee errors and omissions and increased use of mobile devices with vulnerabilities. One threat involving the human factor that is not rated in the top three threats is the use of social media.

A likely reason for this is that many organizations that have been interviewed do not make intensive use of social media**,** but this might provide a false sense of security. Employees are active on social media. Do you know which personal/private expressions or activities are a cyber risk to your organization?

From push to pull – cyber security as a business concern

The keyword when it comes to the human factor in Cyber Security is awareness. An important indicator of awareness in organizations is the frequency with which employees approach the responsible colleague (e.g. CISO) with questions or concerns. During interviews we asked interviewees whether the workforce actively engages the responsible role for cyber security. Although a high number of interviewees indicates that colleagues do actively approach the CISO role in their day-to-day work, there is also a large portion of the organizations that indicate that this is rarely the case or not done at all, and that in most cases the colleague(s) responsible for cyber security need to push information to the workforce.

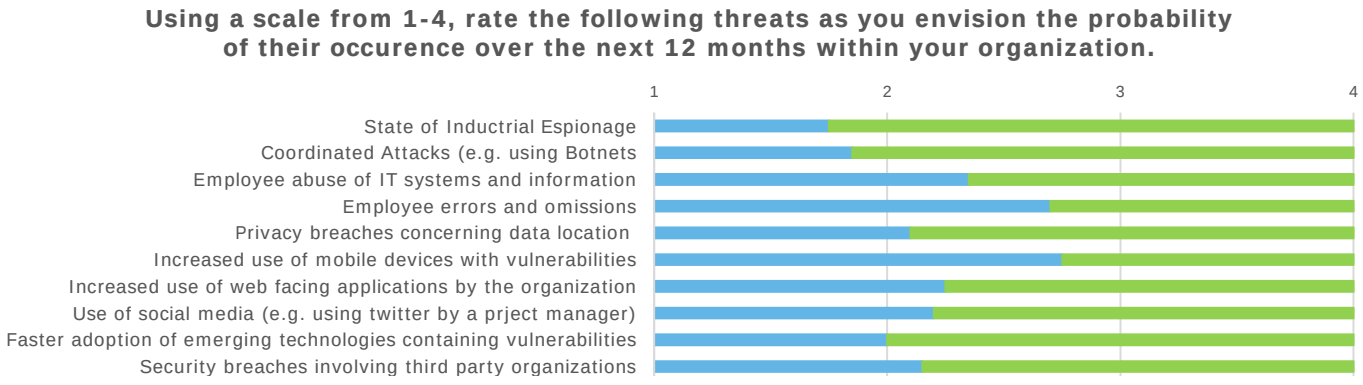


Figure 5: Threat landscape

Building Awareness
There are multiple ways to increase the awareness of your employees on the topic of Cyber Security. Some examples are mentioned below.

Awareness training
The results of this study show that only a little over half of the organizations interviewed provide Cyber Security awareness training to their employees (see figure 6). Awareness training is a very effective way to inform employees of the red flags, and to keep an eye out for and the impact that certain actions may have. Such a training will not only reduce the chance of an incident caused by unawareness, but will also trigger employees to actively think about security in their daily work.

Figure 6: Does your organization provide cyber security awareness training to employees?

Phishing simulation
Phishing is becoming increasingly sophisticated. 'Mass-phishing, which is easily detected by spam filters or recognized by employees, has been replaced with targeted 'spear-phishing' campaigns. Cyber criminals put a lot of effort in making their messages look legitimate, gaining your trust and tricking you into clicking a link, providing data or transferring funds. With Phishing simulation organizations mimic a phishing campaign. This method helps employees recognize what phishing techniques are used and at the same time provides your organization insight into the level of awareness of your organization.

Red Teaming
A relatively new method of testing the resilience of your organization and awareness of your employees is Red Teaming. This method allows organizations to assess their cyber readiness and awareness through scenario based controlled incidents. Undercover reconnaissance, social engineering, infiltration on both physical and technological level, sending of phishing e-mails and investigating your digital footprint all are combined into one.

Red Teaming can be divided into different types of approaches and techniques, such as:

- *Adversarial simulation*
  A realistic scenario based attack, in which security capabilities and awareness levels in regards to the Cyber, Physical and Human aspects are assessed;
- *Advanced Ethical Hacking*
  An advanced form of ethical hacking, which extends beyond scanning your network and identifying vulnerabilities.
- *Intelligence Analysis*
  Intelligence Analysis identifies what an adversary can, externally, identify about you and your organization.
- *Compromise Assessment*
  If you want to catch a thief, think like a thief. This is a combined Blue and Red Team technique in which the combined forces are trying to locate the presence of a potential hacker while at the same time they are working towards eradicating them.

Cyber Security budget

While at the moment organizations in the Dutch Caribbean on average spend between 4% and 9% of their IT budget on Cyber Security, many organizations across all industries indicate that they expect this will be increasing rapidly in the upcoming years. This trend goes hand in hand with an increasing need for having a clearly defined strategy for the Cyber Security budget.

The survey results underline that the budget for Cyber Security is one of the biggest struggles for organizations that participated. Figure 4 shows that the Cyber Security budget is indicated as the biggest barrier in achieving Cyber Security. In many cases we experienced that the question 'What percentage of your IT budget is spent on Cyber Security?' was not an easy answer. The budget for Cyber Security is often not defined as a separate budget from the overall IT budget and is being spent ad-hoc. The biggest problem still seems convincing the board (or upper management) of the importance of spending money on Cyber Security. Organizations struggle to quantify the risks versus the rewards for investments in order to build a convincing case. Again this emphasizes the need for a crystal clear storyline for the C-suite.

Areas of investment

As part of a comprehensive proper Cyber Risk assessment organizations should be able to create a clear view on the most valuable assets protect and therefore prioritize budget requirements based upon such an assessment. Since certain cyber security activities require (significant) investments it is wise to take provisions in case of any business disruption (incident response and recovery), but don't forget about preventive measures (e.g. workforce awareness). While a large share of the Cyber Security budget is currently spent on firewalls and similar security technologies, there are several other areas which require attention, also given global good practices. These topics could include:

- Having a dedicated role for Cyber Security;
- Training of your Cyber Security professionals, but also other departments on Cyber Security (e.g. Lines of Business, Risk and Internal Audit);
- Monitoring technology that helps detection of attacks keeps cyber criminals from dwelling on your company network;
- Assessments in order to get a good understanding of your current security posture;
- Awareness training and other awareness activities for your employees.

Changes in budget towards the future

As many organizations are indicating that their budget for Cyber Security will significantly increase, it is of utmost importance for organizations to have a good understanding of what cyber security risks they identify for themselves, determining what appropriate responses to these risks should be and take precautionary measures. For each cyber risk a provision should be taken to ensure that in case a risk materializes, budget is available for recovery activities.

Threats, incidents and attacks

For some around us the fundamental assertion is that we are at war, a cyber war to be precise. The topic is expansive and seems to become more inclusive every day as the word “cyber” enters almost every aspect of our professional and private life.

With all technological developments and the impact these have on the attack surface of most organizations deploying new technologies, they should realize that breaches are inevitable – and that no industry or organization is immune.

Vulnerabilities

In general, the harsh reality is that a lot of organizations are no match for their adversaries in the cyber domain. Although this stays difficult to address or prove since information sharing on cyber security breaches is still in its infancy. Given this context it’s a given we will have vulnerabilities and the number will probably only increase due to the way technology has intertwined with our daily private and business life.

Cyber incidents occurred

Figure 7 shows that almost 90 percent of the participants in the study have experienced malware and viruses attacks. This explains the high level of knowledge and awareness for specific cyber threats and is also reflected in the Cyber Security budget where a large share of the budget is spent on firewalls. Almost one third of the respondents has also experienced ransomware attacks. Ransomware is computer malware that installs on a victim’s device, encrypts data which makes it unusable after which a ransom payment is requested to decrypt the data or prevent the cyber criminals from publishing the confidential data. From the figure it can be seen that all forms of attacks included in this survey occur, therefore it is important to defend and monitor for all types of attacks.

Impact of cyber incidents

Surprisingly we found that organizations indicate that they perceive the impact of cyber incidents to be low. This may be the case for the malware and virus incidents that have occurred. However, other attacks such as the misuse of digital identities or the disruption of IT systems (can) have significant impact on business operations of organizations (in the Dutch Caribbean) and thus can have a major impact both financially and reputational. From our experience in the Dutch Caribbean we can confirm that some higher impact incidents have occurred, and these are only the cases that have come to our attention or have actually been identified.

Covert attacks

Interviewees were asked whether they feel comfortable that they are aware of all attacks on their organization. Most of the organizations indicated that they do not feel comfortable that they are fully aware. In the next chapter we will address security monitoring which increases visibility across an organization’s network.

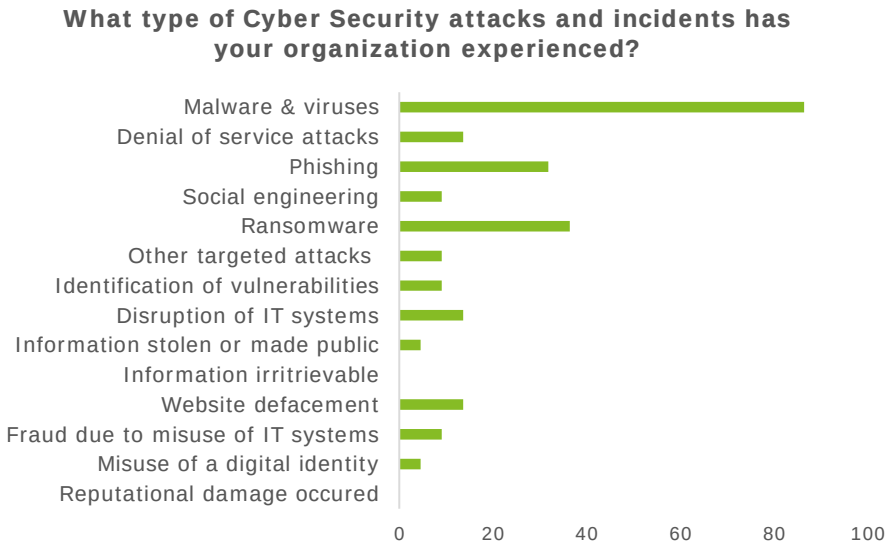


Figure 7: Attacks and incidents

The effects of a cyber-attack can ripple for years, resulting in a wide range of “hidden” costs – many of which are intangible impacts tied to reputation damage, operational disruption, or loss of proprietary information or other strategic assets.

Towards detection

"Why didn't *we* detect it?" That's the all-too-common question when a major cyber incident is discovered – or often, announced by the media.

As IT infrastructures become more complex, this creates exponentially more gaps and weaknesses for cyber criminals to exploit—and allows more ways to evade detection. A risk-focused monitoring capability enables organizations to advance their business strategies more freely—and more safely. Awareness has grown on the fact that cyber incidents cannot be prevented fully, so it is key to have such a monitoring capability in place.

Monitoring of IT assets can be done in different ways. Not all organizations will have the scale and resources to set up a full spectrum Security Operations Center (SOC). Some organizations may prefer to outsource monitoring or assessment activities to external parties that have special expertise for this. Either way monitoring of your IT assets at some level, in some way, is key in detecting cyber-attacks and preventing them from turning into a crisis.

Monitoring and security in the Dutch Caribbean

During our research we asked organizations about two types of methods to realize security: through use of security technologies and by means of the deployment of assessments.

The most commonly used technologies are the desktop and network related technologies (e.g. firewalls, content filtering, anti-viruses. Less used technologies are access and mobile related technologies.

There are different types of assessments that can be performed in order to increase an organization's cyber security posture. The most commonly used assessments in the Dutch Caribbean are version checks of security software and external audits. Internal audits can also be an effective manner to increase the quality of your security overall, having the internal audit focused on Cyber Security specifically can be very beneficial. Effective assessments that are not so commonly used in the Dutch Caribbean are penetration testing and Red Teaming.

Finally, sources for security monitoring used in the Dutch Caribbean are shown in figure 8. Publically available data on Cyber Security trends and red flags are not widely used and could be a useful source to determine monitoring focus.

Which sources are used for security monitoring?

Review network activities	76.9%
Review application logs	69.2%
Review incidents	73.1%
Publically available data	42.3%

Figure 8, sources for monitoring

Third party security

The use of third parties, for example with third-party cloud providers, can leave an organization with sizeable blind spots. One of the biggest challenges organizations face is gaining a thorough understanding of their third-party relationships and the associated risks. Executive management should ensure that third-party risks are included in its overall risk assessment and that sufficient measures are in place to enable the organization to manage all of the risks in its value chain. Different methods to manage third party risks are the following:

- Identifying risks related to third parties as part of cyber risk assessments;
- Adress Cyber Security issues in the contract
- Sign confidentiality and/or Non-Disclosure Agreements;
- Impose your security policy and controls on third parties;
- Where allowed, perform background verification checks on select high-risk, third party eployees;
- Control what access third parties have to your systems and data;
- Perform random spot checks of third parties' sites;
- Require some form of independent attestation.

How does the Dutch Caribbean manage third party risks?

Survey results show that too many organizations are not aware of the security measures that third parties have in place. Most organizations use confidentiality agreements to ensure security with regards to third parties and many organizations also control third parties access. However, very few organizations have identified risks or perform regular monitoring or review activities. Overall, organizations in the Dutch Caribbean need to gain more control over their third parties security, since the supply chain is one of the most frequent attack vectors to breach organizations.

Mobile devices

Mobile communications are an increasingly integral part of the everyday lives of people, both at work as in their private life. As mobile access and options have grown, so have mobile security threats. Such threats are lucrative for hackers and frustrating for individuals and companies.

Corporate mobility offering
Most of the organizations allow private phones for business use (e.g. corporate e-mail), others provide corporate phones to certain employees (in most cases management). This type of mobility is accompanied with new types of risks at device, application, and infrastructure level; thereby requiring changes in the corporate security policy and strategy. How do organizations in the Dutch Caribbean deal with this?

Some risks get riskier
Risks related to mobile phone usage fall into the following main categories:

1) Operational risks: existing security and IT resources and infrastructure are not sufficient to mitigate the risks. Organizations will need to invest in developing technical capabilities and operational processes to support a 'mobility infrastructure'.

2) Technology and data: The following issues can weaken security controls and thus may lead to vulnerable devices and potential loss of data. In addition network connected devices with weak protection can function as a point of entry for cyber criminals.

- end-user modification of device security parameters;
- installing unapproved or corrupt applications with malicious code;
- devices and memory cards with weak encryption;
- mobile OS patching/updating/jail-brekaing;

3) Legal and regulatory: the device or carrier distributors may not be able to meet corporate security requirements. Legal considerations such as employment labor laws may impact the overall mobile strategy.

Mobile security measures
If corporate smartphones are provided to employees in the Dutch Caribbean, the results of the survey show that a lack of knowledge and awareness of these potential risks and prevention methods cause anxiety with corporate management. Most of the interviewed organisations rate the threat of increased usage of mobile phones with vulnerabilities at 3 on a scale of 4. Typically limited security measures are in place. Methods that are most commonly used to ensure a secure usage of mobile phones are remote wipe and forcing security settings for e-mail usage on the mobile devices as can be seen in figure 9. Most of these measures are solely applied to the corporate devices provided by the organization. Very little security measures are in place for privately owned devices.

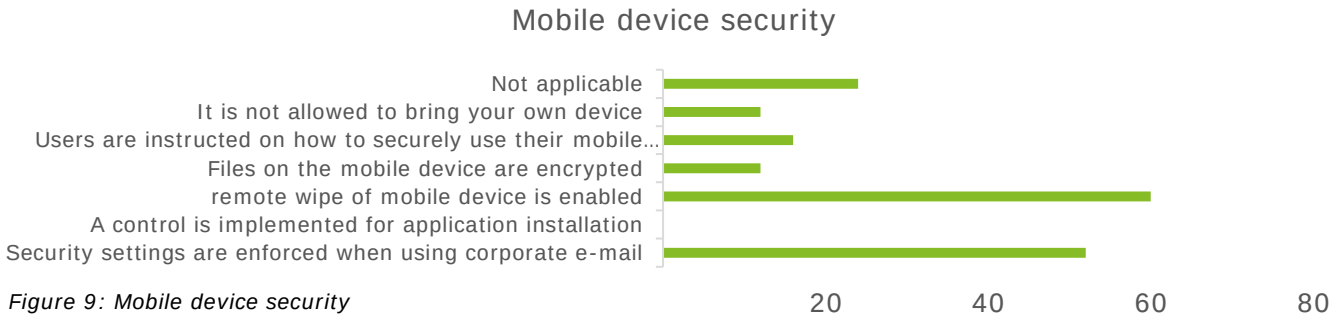


Figure 9: Mobile device security

Privacy

How do organizations protect the personal data of employees and clients? Employees and clients trust organizations when they provide their (confidential and/or personal) information. With regulations for privacy now being in place it is time to start thinking about how to securely handle personal data while taking privacy into account at the same time.

While privacy has been an important topic for a while in other regions in the world (e.g. Europe and US), with regulations now being heavily enforced, it is also becoming increasingly important in the Dutch Caribbean. People are becoming more aware of their rights and it will not be long before the regulations will be enforced on organizations.

This study sheds light on the fact that most of the organizations feel equipped to handle private and sensitive information. However, the methods that organizations use to protect themselves often are limited to managing access roles and privileges, and physically protecting data. A data risk analysis or privacy program are almost never in place.

How to protect personal data
Three important guidelines can help organizations in establishing a safe environment for personal data:

Data management is essential to avoid privacy breaches.
Accountability requires insight and insight is only possible with data management. Such insight requires organizations to draw relationships between (sensitive) data and processes in order to determine privacy requirements and focus, both from a process and IT perspective.

Safeguard your data in a risk-based manner.
Performing risk assessments with a focus on processing, storage and destruction of personal data in your organization is pivotal. Organizations should only store what is really required and destroy data when it is no longer needed, taking regulatory data retention requirements into account

Protecting personal data will help organizations build trust with clients and safeguard personal information.
If organizations want to know (about) their clients and want to tailor their experience and products, their trust will be a prerequisite.

Privacy Impact Assessment
Privacy Impact Assessments (PIA's) are a means to identify high risks to the privacy rights of individuals when processing their personal data and ensures that an organization can formulate measures to address these risks. The PIA should focus on assessing what personal data is processed, what risks this brings along and what measures are in place to avoid breaches of applicable privacy laws.

Privacy regulations in the Dutch Caribbean
Aruba, Bonaire and Curaçao have similar sets of privacy regulations that apply to the handling of personal data. Although not generally enforced yet, we expect this to happen sooner rather than later.

"The respect for the privacy of every human being is a fundamental right in the 'Staatsregeling van het Koninkrijk'."

Per October 1st 2013 the 'Landsverordening bescherming persoonsgegevens (Lbp) has become effective on Curaçao. With the Lbp the responsibility for privacy is no longer with the citizen. The law defines in detail which conditions need to be met for handling personal data. An independent governing body, the 'College Bescherming Persoonsgegevens' is responsible for monitoring compliance with the Lbp.

Business Continuity Management (BCM)

A crisis or an incident can hit anytime and can come from many directions. In many occasions organizations do not have any control over it. The only thing that organizations can do is to be prepared. Ensure that the impact is minimized and continuity of business operations is guaranteed.

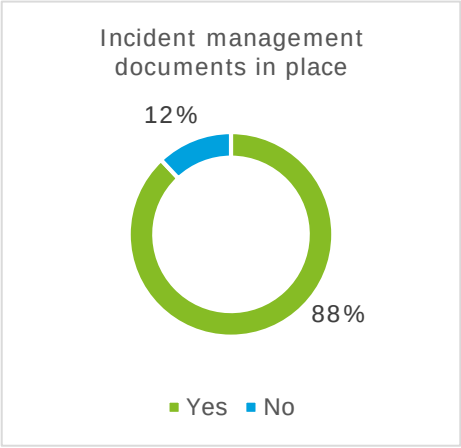
Business need for Cyber Security
Organizations face the prospect of a disruption to buildings, equipment, technology, human resources and third party continuity. A multitude of causes can drive this, such as natural disasters, man made mistakes and increased regulations. To minimize the impact of such a disruption, business leadership teams should work closely and frequently to adequately anticipate and plan for such an event. Protecting critical assets that support the business processes provides the basis for a sound business continuity capability and a resilient enterprise.

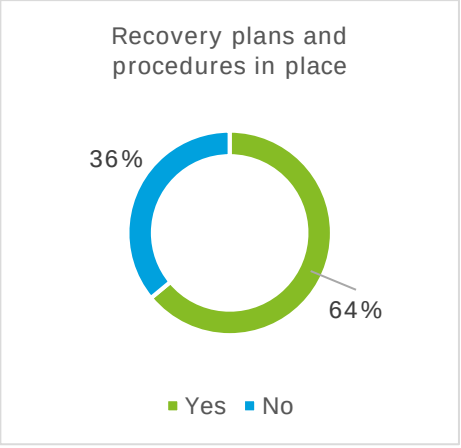
From reactive, recovery based to proactive, risk based.
BCM is about much more than backing up and restoring data to and from tapes, in fact it is about ensuring that your products and services of your business, are available to clients, even when your business is in the midst of an unplanned disruption. Furthermore, BCM can provide you a competitive advantage because you are prepare where your competitors may not be.

BCM documents in place, improvement needed.
The graphs in figure 10 show that most organizations in the Dutch Caribbean have certain BCM documents in place. However, they do indicate that these documents are not always complete and up to date.

By regularly training crisis management teams, performing (operational) risk assessments, testing business continuity and IT relocation plans and increasing employee awareness organizations and its employees are already better prepared in case of a business disruption.

"Prevention is an important first step; however, no organization can be 100% safe from attack. Robust detection and advance preparation and planning may help stop a breach from turning into a crisis."





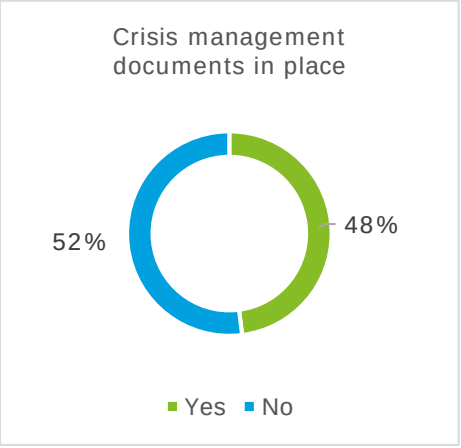


Figure 10: Incident management, recovery plans and crisis management

Secure, Vigilant and Resilient

Yesterday's IT-based security program was often perceived as a burden. Pitted against progress, it too often resulted either in recklessly risky innovation, or opportunities lost to excessive caution. A broader program that is built to position the organization to be secure, vigilant and resilient, rather than simply secure, can help organizations become more confident in their ability to reap the value of their strategic investments.

The interest in and the urgency of the topic of Cyber Security in the Dutch Caribbean is increasing rapidly. The awareness that the Dutch Caribbean is not immune to cyber-attacks and incidents and that these threats are spread over all industries is becoming clearer than ever before.

Organizations are ready to start the battle against Cyber-crime, but many organizations are unsure where to focus there (initial) efforts. 100% secure is a non-existent state and therefore, it is key for organizations to focus on the topics that mostly impact them. Organizations need to gain a thorough understanding of the threats that are specifically applicable for their organization or industry and apply a risk-based approach of determining which assets are most valuable and need protection the most.

Where to start?
For organizations it is important to move from a traditional, standards-driven IT security program to a comprehensive cyber risk program. In order to move into this direction the following steps should be undertaken[1]:

- **Put a senior executive at the helm.** The person in charge of the cyber risk program should be able to lead and command respect among a wide range of leaders at the board level.
- **Map threats to the business assets that matter.** Set the organization's risk appetite and prioritize program areas that contribute to becoming secure, vigilant and resilient.
- **Launch priority projects for early "wins".** Focus on areas or pilot initiatives that directly impact business success or mission achievement, with objectives that can be measured.
- **Accelerate behavioral change through incentives and experience-based awareness.** In addition to traditional security training, provide active learning scenarios that deepen understanding of the impact of day-to-day activity on the organization's cyber risk posture, and identify visible opportunities to reinforce the right behavior through programs that reward speaking up, raising questions and achieving core program objectives.

Secure, vigilant and resilient are the key words to remember:

Secure
Establishing the foundation and building the defences … means embedding good cyber behavior and having risk-prioritized controls to defend critical assets and data against known and emerging threats.

Vigilant
Analyzing threats & identifying issues … means having threat intelligence, and vulnerability and situational awareness to identify and anticipate harmful behavior. This includes security awareness.

Resilient
Respond effectively … means being prepared and having the ability to manage and recover from cyber incidents in coordinated, responsible and timely manner.

[1] With Cyber Risk, Secure, Vigilant and Resilitien are the Watchwords – Deloitte - Edward Powers.

Deloitte's Global Cyber Strategy Framework

In order for organizations to gain a better insight into their Cyber Security stature Deloitte has developed a Cyber Strategy Framework (CSF). Deloitte's CSF allows organizations to better understand the cyber risks they face and their ability to combat the threats applicable in their organization-specific threat landscape. This understanding of your context can be leveraged in powerful what-if analyses.

The diagram in figure 11 provides an overview of the different dimensions of the framework. Each of these will need to be considered when performing a current state assessment and determining the future state considering your organizations required/desired cyber security maturity ambitions.

The framework uses a maturity model ranging from the most rudimentary stage (level 1) to cutting edge cyber security (level 5). The framework utilizes multiple industry standards to which it is mapped (e.g. ISO27001, SANS Critical Controls, NIST Cyber Security Framework and ISF).

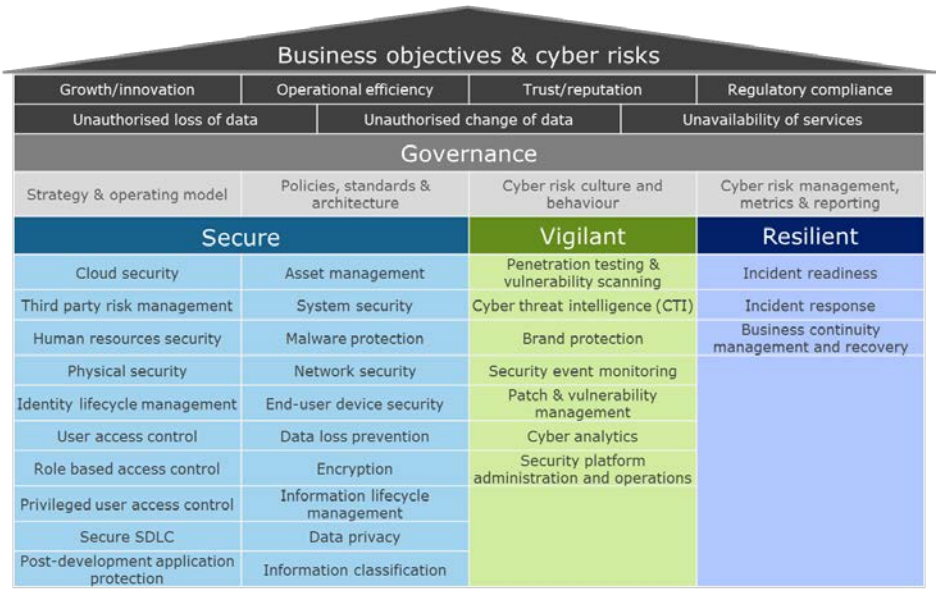


Figure 11: Deloitte's Global Cyber Strategy Framework (CSF)

Understand your company threat landscape

Focus on the right priorities

Understand current maturity level of cyber capabilities

Enhance value from cyber security investments

Develop cyber strategy roadmap

Contacts

Mario Flores
Partner, Risk Advisory
marioflores@deloitte.cw

D: +599 9 433 3353
D: +297 528 6200
M: +599 9 690 8600

Roy Jansen
Director, Risk Advisory
rojansen@deloitte.cw

D: +599 9 433 3313
D: +297 528 6200
M: +599 9 685 6184

Deloitte.