RSSC Revue, "Toward a Secure Cyber Space", Issue 01, September-2014
ISSN xxxx-xxxx

CSIRT, a must have instrument to promote cybersecurity

Perpetus Jacques Houngbo

Abstract— Professionals of the information security find themselves very often in awkward situations where they have to demonstrate the values of their activities to the leaders of their organizations. If they do not succeed, this paves the way for a lot of disappointments and damages which cost the maximum to organizations when security incidents happen. This article aims at reminding the necessity of aligning the objectives of information security on the foundations of the business. It will particularly stress on the implementation and operation of Computer Security Incident Response Team (CSIRT) as inescapable instrument when thinking of resilience, of sustainable development.

Index Terms— Information security, business, cyber secuirty, threat, CSIRT, CERT, strategy.

1. INTRODUCTION

INFORMATION security professionals usally experience hard time trying to advocate for their organization to embark in information security. The domain is often viewed by organizations as hassle or burden bolted on them. This creates cases where information security can hardly deliver all its best. And for it to actually deliver its best, information security has to be infused into the organization.

"Information Security as a business enabler" is the mantra of numerous IT events these days and amidst many recent securities breaches that are disclosed in newspapers, the misfortune of TARGET[1][2] is one of the major illustrations of what could happen in cases where information security is not tackled as a business problem. As said Steve Durbin, global vice-president of the Information Security Forum, "If there was any remaining doubt, this clearly demonstrates that security is a business issue and must be taken seriously by boards"[3].

This paper is an attempt to remind information security professionals, leaders and high profile managers, how tight the business is with information security, and moreover, how they can see that value information security is adding to the business.

This paper will also remind that, nationwide, the concern of cybersecurity is driving similar focuses. At that level, the issue is much more than an operational one. A nation must think of a holistic strategy where information security is a financial investment for the anticipated future: the nature of threats is evolving and a Computer Security Incident Response Team (CSIRT) is one of the great instruments that will complement the national strategy to promote cybersecurity.

This article is built up around two main section:

- the first section will re-explain how information security is business enabler: network infrastructure and information are vital for business and information security highly takes care of them, in line with the primary drivers for business
- the second section stresses on the fact that evolution of the landscape of cyberthreats puts large parts of information security at the level of Computer Security Incident Response Team (CSIRT)

2. INFORMATION SECURITY AS A BUSINESS ENABLER

A. Vital media and vital substance: the network and the data

In today's global economy, nearly every single business is practicing enterprise information management. Based on products and services, there are customers, suppliers, ledgers, e-mails, memos, manuals, web sites, orders, contracts, etc. It is hard to think of any business that does not rely on data and on a network infrastructure that handle the smooth circulation of those data. Most if not all daily operations rely on a network infrastructure: data exchange within all components of the organization at the same premise or all over around the world. The same apply for communications with cutomers, with providers, with partners, with governmental bodies, etc.

Network infrastructure is covering the same vital role in citizen's life as they rely on that infrastructure for simple voice communication but more and more for diverse kinds of interaction with companies, public administration and civil society. Not to mention the paramount place of social network in modern societies.

Network infrastructure is sometimes said to be for business what blood vessels are for human body: an intricate mesh of tubes that transport data (blood for human body).

The material that network infrastructure is transporting for business is totally virtual; the data travelling along the cables are transformed in information that different (individuals and processes) actors use. The same way no human body can expect to survive without blood, the same way no organization can think of its business without the information it will process in order to achieve its goals.

Keeping in mind that network infrastructure is the "cardiovascular" system of the business implies that its design, implementation, monitoring must be handled throughout a robust strategic vision. It is not too much to add that the criticality of the network infrastructure is so high that some countries

- *Perpetus Jacques Houngbo is member of the Executive Team of AfricaCERT where he is in charge of Development Program and also serves as Instructor,jacques.houngbo@africacert.org*

are manoeuvring to control it completely. In August 2010, William J. Lynn, Deputy Defense Secretary of the U.S. said "the best-laid plans for defending military networks will matter little if civilian infrastructure — which could be directly targeted in a military conflict or held hostage and used as a bargaining chip against the U.S. government — is not secure"[4].

Information security is all about taking care of that vital media, the vital material that it transports and people accessing and using them.

B. Primary drivers for the business

The previous paragraph has evoked that network infrastructure is vital for the business. Before gearing towards information security as bisuness enabler, let us review the primary drivers of the business.

When talking about the primary drivers of the business, one must think of the shaping forces that decide (or justify) why the business is being ruled. Eventhough major brands and high profile media can create fashion and push "needs" by forging and leading opinions, the world today is accelerated by consumers. They are the one driving demands for specific products and services, and business adapts by becoming not just product centric or services centric but more consumers centric.

With customers in mind, the main driver that is undoubtly mentioned about business is finance. It is followed by other elements like market position, growth (customers / corporate), responsibility. Those are the four categories of primary drivers for business that will be referred to in this paper. That compilation of globally accepted primary drivers for the business is built around a real life situation of customer-centric business transformation[5, pp. 282–285] and the study performed by [6].

Finance is the most important and most obvious driver of the business. Investing a lot of resources (financial, human, organizational, etc.) is driven by the anticipated return from the business.

Market position is very important as well. It encompasses elements like protection of the brand and name, maintaining the quality and reputation of products and services, foreseeing change in environmental factors and adapting to them.

Growth comes next. Growth pairs with continuity of the organization, with improvement in business processes.

Responsibility is in multiple dimensions. It goes to diverses actors: to shareholders, to society, to employees, to country.

A savvy manager continuously focuses on those drivers and derives them into indicators that he monitors. In the highest position within an organization, the main duty of the manager is setting strategy and vision. The manager's decisions include items like markets the company will enter, competitors to challenge, products lines to offer, ways of differentiation, mean of protection and promotion of brand, etc. After hiring the right team that matches her vision, those who will champion the culture of the organization, that highest in rank make work done through people, by actionning levers: budgets, partnerships, programs, etc.

It is not superfluous to note that when talking of business, this paper not only refers to private companies, but also to civil society and to governemental activities as well.

The paper will then present in the following paragraphs how information security must be aligned to those business goals.

C. Aligning information security to the business goals

Let's assume that a company, a bank for instance, wants to implement a resilient information system with the high expectation to generate competitive advantage on it. The company wants to use that resilience in its marketing to attract and maintain customers. In that case, a professional of information security can easily sell the concept of business continuity and all its components to the senior management of that company. That is the exercice this paper will perform in the next paragraphs.

Roughly taken, finance as primary driver for the business equates to increase in profits, which translates into increasing revenues and decreasing costs. This is basically achieved by exploitation of the organization's information[7]. It is then of paramount importance to have information available, when needed, for those who have been granted the privileges of accessing it: that is part of the aims of information security, more specifically of access control.

As evoked in the previous lines, information is a high value asset for the business as well as the network infrastructure that facilitates access and use of that information. It is with those two instruments that business develops loyalty of current customers, gain more new customers, interact with them, market products and services, partner with other business, etc. That is the reason why access control is definitely a "must have" for any business. And access control is one of the components of the complex field of information security.

Access control, as defined by (ISC)² CBK[8] as the process of allowing only authorized users, programs, or other computer systems (i.e. networks) to observe, modify, or otherwise take possession of the resources of a computer system. Implementation of access control is using a set of mechanisms to protect the assets of the information system.

The purpose of information security is to preserve:

- **Confidentiality** - Data is only accessed by those with the right to view the data.
- **Integrity** - Data can be relied upon to be accurate and processed correctly.
- **Availability** -Data can be accessed when needed.

The paper will rely on the ten domains defined by (ISC)² CBK[8] for implementation information security:

- **Access control**: collection of mechanisms that work together to create security architecture to protect the assets of the information system. They ensure the system's availability, confidentiality, and integrity.
- **Telecommunications and network security**: network structures, transmission methods, transport formats and security measures used to provide availability, integrity and confidentiality.
- **Information security governance and risk management**: identification of an organization's information assets and the development, documenta-

tion and implementation of policies, standards, procedures and guidelines.
- **Software development security**: controls included within systems and applications software and the steps used in their development.
- **Cryptography**: principles, means and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Security architecture and design**: concepts, principles, structures and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity and availability.
- **Security operations**: identification of the controls over hardware, media and the operators with access privileges to any of these resources.
- **Business continuity and disaster recovery planning**: preservation of the business in the face of major disruptions to normal business operations.
- **Legal, regulations, investigations and compliance**:
  - computer crime laws and regulations
  - investigative measures and techniques used to determine if a crime has been committed and methods to gather evidence.
- **Physical (environmental) security**:
  - threats, vulnerabilities of the physical environment
  - countermeasures utilized to physically protect an enterprise's resources and sensitive information.

The following will list, for each primary driver of the business, the domains that are more inclined to directly contribute to the goals of the driver. The identified domains are obviously not the only one, but the more inclined to contribute.

Finance

Business goals
- Increase in revenue
- Decrease in or control of costs
- Extension of customers base

Information security domains
- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Security Architecture and Design

Market position

Business goals
- Protection of the brand and name
- Quality and reputation of products and services
- Foreseeing change in environmental factors and adapting to them

Information security domains
- Access Control
- Telecommunications and Network Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

Growth

Business goals
- Continuity of the organization
- Improvement in business processes

Information security domains
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Security Architecture and Design
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance

Responsibility

Business goals
- Wealth for shareholders, employees, customers and society at large
- Long-term value and performance for stakeholders (investors, clients, employees and society)
- Meaningful jobs
- Respect for the individual employee
- Commitment to customer service
- Achieving excellence
- Promotion of environmental and human rights concerns

Information security domains
- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

"access control" is almost everywhere and all ten domains are involved in the diverse responsibilities of the business.

3. CSIRT TO COMPLEMENT CYBERSECURITY INSTRUMENTS

A. Understanding the new scheme of threats

At this point, this paper is expected to have made clear connections from the business to information security. It wants next to present an overview of the current scheme of threats to information systems with the intention to stress more on the imperative necessity to understand how information security, by protecting against those threats, is warranting an environ-

ment that is favourable for the business.

The current landscape of cyberthreats is a mix of bad news[9] and good news. Viruses are still in the place, with their burden of enoyances. Worms have increased their capacity to spread and are inflicting damages at larger scales. All those malware have drastically improved their capacities to organize money stealing and intrusion in privacy. Scarier is the fact that they are performing on all type of devices within any kind of network infrastructure.

Fortunately there is good news, some "positive developments"[10] have been observed:

- successes by law-enforcement
- increase in reports and data regarding cyberthreats
- stronger awareness and then better response to threats and vulnerabilities
- increased cooperation among relevant organisations.

Business seems to be operating a transformation "to a **secure, vigilant, and resilient model**"[11]. At least business must operate that transformation if it wants to sustain activities.

The traditional focus on being secure only protects "against known and emerging threats, comply with industry cybersecurity standards and regulations". Today's needs are to "be vigilant" which means to be able to "detect violations and anomalies through better situational awareness across the environment". And best if the business can reach the "be resilient" stage. At that stage, business has established "the ability to quickly return to normal operations and repair damage".

"**Being secure**" is what every single business is supposed to do as its minimum effort in enabling business with information security. "**Being vigilant**" already calls on a higher level as it implies elements like:

- technology Watch
- security audits or assessments: infrastructure review, best practice review, scanning, penetration testing
- intrusion detection services
- information dissemination.

One can see that those elements are more or less the services that a computer security incident response team (CSIRT) is offering, in the category of proactive services. The objectives of those services is to reduce the number of incidents and also to reduce their impacts when they happen. These services help prepare, protect, and secure information systems in anticipation of attacks, problems, or events.

The "**Being resilient**" goes further. Quickly returning to normal operation and repairing damages suppose that some specific capabilities are in place, that security quality management is enforced. Once again, this is part of services offered by CSIRT in improving overall security, services that encompass:

- risk analysis
- business continuity and disaster recovery planning
- security consulting
- awareness building
- education / training
- product evaluation or certification.

The response that business must give to the evolution of the cyberthreats includes necessarily implementation and operation of CSIRTs. They are part of the arsenal that will help business reach its objectives by realizing the model of security, vigilance and resilience.

B. CSIRT to complement cybersecurity instruments

Defining cybersecurity is a hard task this paper will not try to do. What matters is reminding that cybersecurity encompasses many parts: technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. We will then accept cybersecurity as defined by the ITU Recommendation X.1205 (04/08). "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*"[12]

Authors often stress on the coordinated efforts that cybersecurity requires. And CSIRTs are particularly effective on that aspect of coordination of efforts from different bodies. Implications of vigilance and resilience as elaborated in previous paragraphs stress more on the needs for CSIRT.

CSIRT is "a must have", not just a nice instrument among the battery of weapons available to enforce cybersecurity.

4. CONCLUSION

Business creates value for stakeholders, for employees, for the community, for the country. Today's business is so tightly connected with information systems that information security is directly contributing to business objectives. Network infrastructure and information are vital for business and information security highly takes care of them, in line with the primary drivers for business

The evolution of the landscape of cyberthreats is impulsing to a new response from the business. It must operate the transformation "to a **secure, vigilant, and resilient model**". A computer security incident response team (CSIRT) offers a battery of services that encompasses detections of violations and anomalies, capacities to quickly repair damages, straightforward return to normal operations and recovery. CSIRT is an essential piece of the organization to be implemented for that model to succeed. **CSIRT is "a must have".**

5. REFERENCES

[1] "The Target Breach, By the Numbers — Krebs on Security." [Online]. Available: http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/. [Accessed: 14-Aug-2014].

[2] "Target Missed Warnings in Epic Hack of Credit Card Data - Businessweek." [Online]. Available: http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[Accessed: 14-Aug-2014].
[3] "Target CEO Exit Highlights Business Side of Security | SecurityWeek.Com." [Online]. Available: http://www.securityweek.com/target-ceo-exit-highlights-business-side-security. [Accessed: 14-Aug-2014].
[4] "U.S. military wants to exert influence over private cyber infrastructure | Network World." [Online]. Available: http://www.networkworld.com/article/2217257/malware-cybercrime/u-s--military-wants-to-exert-influence-over-private-cyber-infrastructure.html. [Accessed: 14-Aug-2014].
[5] K. Krishnan, *Data warehousing in the age of big data*. 2013.
[6] P. Clements and L. Bass, "Business goals as architectural knowledge," in *Proceedings of the 2010 ICSE Workshop on Sharing and Reusing Architectural Knowledge*, 2010, pp. 9–12.
[7] D. Loshin, *Business intelligence the savvy manager's guide*. Waltham, MA: Morgan Kaufmann, 2012.
[8] "$(ISC)^2$ CBK | What is the Common Body of Knowledge." [Online]. Available: https://www.isc2.org/cbk/Default.aspx. [Accessed: 17-Aug-2014].
[9] "How the cyber threat landscape is evolving -- Comodo security [Q&A]." [Online]. Available: http://betanews.com/2014/04/17/how-the-cyber-threat-landscape-is-evolving-comodo-security-qa/. [Accessed: 18-Aug-2014].
[10] "ENISA Threat Landscape 2013." .
[11] "Transforming cybersecurity - New approaches for an evolving threat landscape." .
[12] I. T. S. Sector, "ITU-T Recommendation Z. 120," *Message Sequence Charts (MSC96)*, 1996.