Evolution of National and Corporate CERTs - Trust, the Key Factor

OLAF KRUIDHOF
Capgemini, The Netherlands

Abstract. This paper discusses the evolution of Computer Emergency Response Teams (CERTs) due to trends in technology and society. It shows how these trends affect the selection of services a CERT can provide to its constituency, and the effects on its resources. The argument is that CERTs need to focus more and more on the specific services they can provide. The selection of these services must be driven by the objectives of their parent organization, the constituency they serve, and the urgency by which services must be provided. The paper further asserts that cyber security organizations (highly) specialized in a limited number of tasks should collaborate with others in order to effectively handle incidents. Trust among participants represents the basis for any successful collaboration. Trust, however, only exists between people. Thus, several other elements need to be in place in order to extend individual trust to organizations.

Keywords. Cyber security, computer emergency response teams, information sharing, security services, technology trends, trust building.

1. Introduction

1.1. Document Structure

After a brief definition of some publicly available terms and references, the first section discusses objectives, capabilities, and services of CERTs, types of CERTs, and their evolution. The second section discusses technology trends, including cyber security, and the third section explores their effects on CERT operations. The final section describes ways to gain the trust and respect necessary for successful collaboration between CERTs.

1.2. Terminology

According to the Carnegie Mellon University (CMU) designation, the term CERT (Computer Emergency Response Team) refers to a team of IT security experts whose main business is to respond to computer security incidents — the first team was created in 1988 in response to the Morris Worm incident. The term CERT is a registered service mark of CMU and is licensed to other teams around the world.

As an alternative, the term CSIRT (Computer Security Incident Response Team) also refers to a team of IT security experts designated to respond to computer security incidents. This term, however, is more accurate since it reflects a broader array of security services provided, beyond reactive functions.
Terms like Security Operations Center (SOC) and Network Operations Center (NOC) are also used, mostly in industry. Although their names suggest an operational responsibility, they are often tasked with similar broad duties as a corporate CERT or CSIRT.

The term CERT appears to be more commonly used for national and governmental security teams. Since this paper focuses primarily on (multi-) national or governmental CERT operations, the term CERT is used as an equivalent of CSIRT, SOC and the likes.

1.3. Public Information

Since the first cyber security incident, a significant body of work has been developed on the topic of countering computer security incidents. The Software Engineering Institute (SEI) at Carnegie Mellon University has been and continues to be an important source for literature on defining, establishing and managing CERTs.

In addition, the European Union—and the European Network and Information Security Agency (ENISA) in particular—has developed a large collection of material to guide member states in creating and running national cyber security centers, and ways to encourage collaboration between them.

In various other countries around the world, such as in the Asia Pacific and South America regions, CERTs have been established, and guidance and lessons learned from their operations have been documented.

The volume of existing literature illustrates the importance of cyber security as a topic and the scale of initiatives undertaken worldwide to handle threats and incidents.

The vast majority of CERT-related information available provides useful guidance for establishing governmental and national CERT initiatives. Clearly, trade and industry are also spending significant amounts of time and money on cyber security incident responses. However, little information is available from an industry perspective about the creation and functioning of CERTs. Most of the publicly available industry information on cyber security stems from security companies that offer commercial services and products to handle cyber threats and incidents (e.g. Symantec, Kaspersky, McAfee, etc).

For obvious reasons, virtually no information is available on the activities of operational CERTs, whether national, governmental or industrial. Some useful information on collaborations between CERTs and information sharing bodies is available through other organizations such as Information Sharing and Analysis Centers (ISACs). Considering the dynamism of the cyber security field and all available sources, this paper prioritizes the more recent information.

2. CERT Operations

A well-functioning CERT should provide a carefully selected set of services to its well-defined constituency (customers) in order to fulfill the mission of its parent organization. As shown in the past 25 years, it is not sufficient for a CERT to bring together a group of IT security experts and task them with providing certain services. A CERT needs to be a well-prepared, well-equipped, and well-managed organization. Therefore, a management structure, support structure, and clear mandate are also key capabilities that must be put in place.
ENISA identified a set of baseline capabilities for national and governmental CERTs.[1] These capabilities are categorized into four areas:

- **Mandate & Strategy** — the powers and justifications detailed in a strategic document on cyber security granted by the respective government to the team;
- **Service portfolio** — the services that a team provides to its constituencies or that it uses for its own internal functioning;
- **Operational capabilities** — the technical and operational requirements that a team must comply with; and
- **Cooperation capabilities** — requirements on information sharing with other teams. This may be partly covered by the previous three categories.

These areas are very similar to the elements in the CSIRT Framework, designed by CMU/SEI.[2]

When setting up a CERT, these four capability areas should be addressed consistently. Typically, the first step in creating a CERT is to establish its mandate and strategy and use that in the second step to derive the required service portfolio. In step three, the service portfolio should help define the necessary operational and cooperation capabilities. However, this should be a cyclical process, where the service portfolio (i.e. the results that can be delivered) influences the mandate and strategy, the operational capabilities determines the feasibility of the services delivered, and so forth.

Two types of cycles can be expected. The first iteration should take place at the incipient stages of a CERT. The capability areas should be addressed at least twice in order to ensure that they are consistent and coherent. Once a CERT is in operation for at least some time, additional iterations through the four areas should be made in order to respond coherently to trends and developments in the cyber domain, and assure that assets are being protected. This evaluation will eventually lead to an evolution of the service portfolio and required capabilities.

### 2.1. Mandate & Strategy

As part of the Mandate & Strategy, CERTs must have a well-defined area of operation, team objectives, audience, and specific types of assets to protect. Although cyber incidents do not respect national borders, the operations of a CERT will be bound by a legal and regulatory framework, which will include the geographical area where a CERT is allowed to operate.

Typically, the objectives for national CERTs are stated in terms of coordination and facilitation with other CERTs within state borders, and cross-domain CERTs nationally and internationally. Governmental CERTs are responsible for the protection of governmental ICT infrastructure, often including critical information infrastructure. As a result, national and governmental CERTs usually serve two types of constituencies. While national CERTs serve a broad audience ranging from the government to private organizations and civilians, the constituency of governmental CERTs consists of government staff that manages government ICT infrastructure.

The differences in objectives and constituencies should shape a CERT’s strategy and evolution for answering the challenges presented by cyber adversaries.
2.2. Service Portfolio

The portfolio of services that is widely used as the de facto set of CERT services has been presented by CMU in 2002.[3] The portfolio is organized in three categories:

- **Proactive Services:** performed before an incident occurs or is detected.
- **Reactive Services:** executed when an incident becomes known.
- **Security Quality Management Services:** continuously executed in order to ensure incidents can be dealt with.

<table>
<thead>
<tr>
<th>Proactive Services</th>
<th>Reactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Announcement</td>
<td>- Alerts and Warnings</td>
<td>- Risk Analysis</td>
</tr>
<tr>
<td>- Technology Watch</td>
<td>- Incident Handling</td>
<td>- Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>- Security Audits or Assessments</td>
<td>- Incident Analysis</td>
<td>- Security Consulting</td>
</tr>
<tr>
<td>- Configuration and Maintenance of Security Tools, Applications, and Infrastructure</td>
<td>- Incident Response on Site</td>
<td>- Awareness Building</td>
</tr>
<tr>
<td>- Development of Security Tools</td>
<td>- Incident Response Support</td>
<td>- Education / Training</td>
</tr>
<tr>
<td>- Intrusion Detection Services</td>
<td>- Incident Response Coordination</td>
<td>- Product Evaluation or Certification</td>
</tr>
<tr>
<td>- Security-Related Information Dissemination</td>
<td>- Vulnerability Handling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Vulnerability Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Vulnerability Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Vulnerability Response Coordination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Artifact Handling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Artifact Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Artifact Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Artifact Response Coordination</td>
<td></td>
</tr>
</tbody>
</table>

In order to select the appropriate combination of services that will allow a CERT to fulfill its mission, the broad objectives stated in the mandate need to be refined. Although this process of refinement will most likely lead to different results for each individual CERT, the following baseline set of objectives that should be included in each CERT’s portfolio is offered:

- Identification of security threats and potential incidents;
- Detection of security threats and incidents;
- Coordination of incident response activities;
- Containment of security incidents;
- Mitigation of security incidents;
- Attribution of security threats and incidents;
- Business Continuity despite security threats; and
- ICT resilience against security threats.
Each of the services in the portfolio serves one or more CERT objectives, and main objectives can be identified for each service. The following table presents a mapping of CERT services and corresponding main objectives which can be used to define a clear focus for selecting services to be provided by each specific CERT. The mapping does not imply that services cannot support other objectives as well. However, the aim is to provide guidance in selecting the most relevant services for any particular CERT.

### Table 2. CERT Services per type of CERT

<table>
<thead>
<tr>
<th>CERT Services' main focus</th>
<th>Identification</th>
<th>Detection</th>
<th>Coordination</th>
<th>Containment</th>
<th>Mitigation</th>
<th>Attribute</th>
<th>Business Continuity</th>
<th>ICT resilience</th>
<th>Coordinating CERT</th>
<th>Servicing CERT</th>
<th>Thematic CERT</th>
<th>Product CERT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Announcements</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Watch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Audits or Assessments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Tools, Applications, and Infrastructures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development of Security Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-Related Information Dissemination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reactive Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alerts and Warnings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident analysis</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response on site</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident response coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact response coordination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Quality Management Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Consulting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness Building</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education/Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Evaluation or Certification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3. Types of CERTs

As discussed above, the Mandate & Strategy of a CERT, and especially its objectives, will define what services a CERT can provide and which constituency it can serve. This allows for the identification of different types of CERTs with different sets of services (see Appendix A – CERT Services per type of CERT).
• **A Coordinating CERT** coordinates cyber security related tasks between more specialized CERTs. In order to achieve this overall objective, a Coordinating CERT is likely to focus on Identification, Coordination, Attribution and Business Continuity. As a result, one may expect the service portfolio of a Coordinating CERT to contain at least the services in the proactive section, several of the ones in the Security Quality Management Services category, and the coordination services in the reactive section.

• **A Servicing CERT** provides proactive and reactive security incident services. A Servicing CERT focuses on handling incidents in various types of IT infrastructure (e.g. critical infrastructures like the power grid, or business infrastructures like a local computer network). A Servicing CERT can be part of an organization where all employees represent its constituency, or it can be a separate organization that provides its services on a commercial basis to one or more companies. The objectives of a Servicing CERT tend to cover the full spectrum of security objectives listed above, either as an in-house organization or as a commercial company. Therefore, a Servicing CERT can be expected to cover the full service portfolio.

• **A Thematic CERT** is a network of collaborating CERTs unified by a particular theme (e.g. ICS-CERT for oil & gas). The main focus of a Thematic CERT is a proactive exchange of information about specific threats and vulnerabilities and how to counter them, supported by theme-specific tools. Thematic CERTs can have arrangements for mutual support in case of a cyber emergency. Similar to a Coordinating CERT, a Thematic CERT is likely to focus on Identification, Coordination, Attribution and Business Continuity. Additionally, a Thematic CERT will support its members by enabling domain-specific Detection, Mitigation and ICT resilience. Achieving the extended set of objectives will require a more elaborate set of services. Other specialized organizations may choose to limit their objectives to information sharing only. Such organizations are often called Information Sharing and Analysis Centers (ISAC). Examples are the US IT-ISAC that aims at being ‘the definitive source for security information impacting the IT Sector’[4] and the European FI-ISAC that shares cyber security information between parties in the financial sector.

• **A Product CERT** focuses on handling security incidents related to a certain (family of) product(s), and is normally provided by the vendor of the product. A vendor will offer security services via a Product CERT to its customers as a mean of assurance that its products will operate as expected. A Product CERT will focus on sharing information concerning threats and vulnerabilities to a specific product and mechanisms to handle incidents and artifacts. In order to fulfill the needs of its constituency, a Product CERT is likely to focus on Identification, Detection, Containment, Mitigation and ICT Resilience. A Product CERT will provide many similar services to a Servicing CERT, albeit that they will be limited to the vendor’s product(s).

2.4. **Evolution of a CERT - Operational and Collaboration Capabilities**

Once a CERT has been established, a common pattern can be identified for the evolution of its operational capabilities. The initial drivers for establishing a CERT
reflect a sense of urgency due to, for example, the increase in the number and severity of computer security incidents, an enhanced cyber security awareness, new laws and regulations for protecting information assets or, as in the case of a Coordinating CERT, the realization that individual organizations cannot provide sufficient protection against cyber threats that affect the general public.

The first stage in creating a CERT is to provide reactive services—the ability to respond to incidents by containing and mitigating threats. Usually, the Servicing CERT of an organization provides such responses on-site. Obviously, the CERT needs to first have the right staff and tools. The tools must be based on the technology used by the constituency, while the staff needs to have the appropriate skill set to understand the technology, the infrastructure, and the tools they use. An investment in staff training is essential. In general, the initial staff will be modest, about 10 to 12 full-time equivalent (FTE). As a preparatory step, CERTs that are successful will have established their own network of trusted partners (e.g. with the Product CERT of the vendor of a key product or technology) that will provide information and support in times of crisis. The base for this type of partnerships is mutual trust; trust between individuals. Responding to an incident requires trustworthy partners that can gain access to the affected ICT infrastructure and are allowed to make modifications using their own tools. This requires trust in the person, his or her abilities, and the tools used. Normally, a screening process and some structures for compartmentalized information sharing are put in place in order to obtain a basic level of formalized trust, but at this stage the bottom line is still trust in people.

The second stage of successful CERTs is building (ICT) resilience against threats and limiting vulnerabilities. The CERT should extend its capabilities in order to detect and analyze vulnerabilities and threats and their potential impact on an organization’s infrastructure. In addition, they should be able to ensure ICT infrastructure resilience, enabling risk analysis and product evaluation or certification. Finally, a learning capability is needed to capture and accumulate the information derived from the various analyses, and make it accessible to the appropriate staff at all times. This requires the staff to have different types of skills. Some staff members need to be highly technical in order to conduct analyses, while others need to have architectural skills to assess the state of the infrastructure and the impact on the compromised individual products. The initial staff would need to be augmented by about 8 to 10 FTE.

In many instances, the required level of technical expertise can only be found at the vendor of the product or technology. This dependency will motivate vendors to set up a Product CERT.

The third stage of a CERT demonstrates a more proactive and preventive behavior. Leveraging the available knowledge, the CERT should become active in promoting awareness and motivating its constituency to apply security measures. At this stage, both the desire and need for organization-wide, and even sector-wide rules and regulation, and the incentive for sharing and exchanging security related information emerge. Indeed, the desire for coordinated research on threats and vulnerabilities to get ahead of the power curve of security attacks grows too. In short, the need for a Coordinating CERT and potentially a Thematic CERT becomes apparent.

Resource requirements would have to change accordingly. Some of the highly specialized technical skills can be provided by a Product CERT. Raising awareness of the wider constituency about security issues requires communication skills more than technical skills. At this stage, the staff would need to be further augmented by four or five FTE who are more business-oriented.
In the fourth stage, CERTs are connected into a network of collaborating CERTs, sometimes only within a single industry. These connections may be coordinated by a Coordinating CERT or linked through a Thematic CERT. At this stage, the collaborating CERTs will be developing what can be achieved by their combined capabilities. Considerations of task specialization are likely to occur.

At this stage, resources will be required to act as liaisons to all the various parties to which a CERT is linked: peer-CERTs, Coordinating CERTs, Thematic CERTs, and Product CERTs. This will require a further increase in resources, depending on the density of the CERT-network.

3. Trends that Increase the Need for CERTs

The operations of organizations are influenced by developments in technology and, as a consequence, in society. This section briefly discusses a series of current technology trends, including their impact on society, and a number of specific cyber security trends.

3.1. Technology Developments

- **Outsourcing** has been a theme in ICT-operations for some time. In general, the opportunities offered by outsourcing are considered from a financial perspective: moving commodity tasks to organizations that offer financial benefits (often labor costs). However, relying on the software, hardware and security procedures of a third party introduces risks that are not easy to manage. If the service providing party is compromised, this might also affect its customers. Even if the internal ICT infrastructure of only one customer is affected there can be a chain effect to the service provider and other customers. Despite the clear agreements on quality of service in service level agreements including security, reflecting the required level of trust, the outsourcing organization cannot apply its own level of rigor in risk and vulnerability analysis, security audits, and protective measures. Mechanisms must be developed to ensure that service providers will always match or outperform the security requirements of their customers.

- **Cloud services**, especially file sharing services, have become popular. The ease of use of cloud services for end-users presents a new risk to an organization’s ICT infrastructure and information policies. The use of processing services, like Software as a Service (SaaS) and Platform as a Service (PaaS), or file sharing services in the cloud can easily allow confidential information to be leaked outside an organization. In order to prevent unauthorized distribution of information outside an organization’s borders, specific measures must be taken to control access to cloud services.

- **Mobile devices** such as tablets and smart phones have become ubiquitous and allow staff to work from any location, including their homes. These devices have various pieces of software embedded and hold a considerable amount of data. Organizations are considering ways to handle them. Strategies like Bring Your Own Device (BYOD) allow employees to bring whatever device (and software) they personally prefer into the organization’s ICT infrastructure. More limiting strategies like Choose Your Own Device (CYOD), which
allows employees to select a device from a limited pre-selected set (sometimes including software), are also being implemented. Each strategy will require its own level of security measures in order to ensure that confidential information and private information are not shared in unintended ways. Due to their nature, these devices can be used outside organizations physical borders, rendering traditional (physical) security measures less effective.

- **Big Data** is a trend resulting from increasing bandwidth and storage capacity at increasingly lower prices. Big Data allows for the discovery of patterns in large collections of data, using statistical techniques. These large volumes of data present a new and valuable asset to both organization and malicious actors alike. Big Data is a new concept that needs to be incorporated in the security policies of an organization. Organizations also need to be aware that others may be collecting Big Data about them. Therefore, information sharing policies need to take this new trend into account as well.

- **The Internet of Things** is emerging as a result of increased connectivity, underpinned by the power of IPv6. Connectivity has increased enormously and has become more and more wireless, using intelligent protocols from the IEEE 802.11-family. Where the traditional Internet is being used in the information realm, the Internet of Things allows for the control of physical objects, ranging from industrial components, like pumps and valves, to washing machines at home, and even parts in cars, such as cruise control. This trend will not only raise new challenges for organizations to address, but will also encourage a discussion on the boundaries of cyber protection. Questions like: ‘Is the role of a CERT limited to its parent organization or should its constituency be extended to the individual civilians?’ will need to be addressed.

In general, organizations continue to become more dependent on their ICT infrastructures, which have become more complex and more connected to other parties. In fact, the role of ICT has evolved from a traditional one – supporting existing manual processes – to one right at the heart of operations. Today, many operations in business and the military cannot be conducted without a reliable ICT infrastructure. This introduces new challenges and growing impacts on the operations of organizations.

### 3.2. Cyber Security Trends

- There is a global increase in awareness of large-scale cyber incidents, as discussed throughout this volume. This is partly due to better detection and information sharing, and partly because the technical means for attacks have become more widely available. The threshold to carry out a cyber attack is now much lower since it is easier to use attack tools, thus decreasing the required skill level of attackers. There are even professional cyber criminals that offer their services and guidance on the Internet–this is cyber crime as a service.

- There is also an increase in the sophistication of cyber attacks. This does not mean that each attack is more complex; rather that existing tools for cyber attacks are being developed further and are becoming more sophisticated and more difficult to counter. As a consequence, tools for detecting and handling cyber threats have shorter life spans and need to become more flexible to
allow for more dynamic responses and continuous updates. Another consequence of this increased sophistication is that attribution is becoming even more difficult. This is especially true for so-called Advanced Persistent Threats (APTs) carried out against governments and large companies, often for espionage purposes.

- In many organizations, managers (C-level) have come to recognize that cyber security is not only a technical issue. They have become aware that in many respects it is cheaper to develop and adopt preventive measures, than employ repair measures, including public communication, after the breach. It has also become clear that such measures need to be implemented structurally rather than as a one-time effort. There is also more pressure from a company’s environment—customers and business partners are demanding trustworthy collaborations, and governments are beginning to introduce regulations that require management action on this topic. Management has also become more aware of insider threats and the fact that current and former employees, who can no longer be trusted, can breach security relatively easily.

4. Effects on Cyber Operations

The trends discussed above result in significant challenges for all organizations connected through cyberspace. Not only have threats grown in number, scope, and sophistication, but even elements in ICT infrastructures have become increasingly diverse and pervasive, and, most importantly, organizations are increasingly dependent on a flawless functioning ICT infrastructure.

4.1. Urgent Need for CERTs

The need for specialized and dedicated units that can respond to cyber security incidents has been evident for quite some time, both at the enterprise level and at the (inter-)national level. Considering the fact that fighting and recovering from cyber incidents cannot be successful as an isolated effort from one organization or even from a single nation, it is very valuable that EU leadership as well as NATO leadership devotes so much effort to stimulating and facilitating the establishment of CERTs by their member states. The recent trends only emphasize the urgency for widespread development of CERTs at all levels of society.

- At the enterprise level, organizations have realized that achieving cyber security is more than a technical problem, and that it requires managerial action and oversight throughout the entire organization as much as rules and software solutions. Effective security has to synthesize organization-wide prevention and mitigation measures, and not only rely on IT professionals working in a vacuum to ‘fix’ a breach after the fact.[5] CERTs can provide proactive and reactive functions, but also preventive and educational services for their constituency within an organization.

- At the national level, there is a clear need to create Coordinating CERTs that can support and facilitate national industry and other governmental bodies in establishing more dedicated Servicing and Thematic CERTs. Many EU and
NATO countries (EU: 23 of 28, NATO: 22 of 26)[6] already have national CERTs in operation, albeit at various levels of maturity.

- At the international level, EU and NATO member states are connected across borders via EU and NATO networks. This calls for governmental Servicing CERTs that protect governmental networks and systems, and prevent the dispersion of attacks to fellow member states. There are also a significant number of countries that have established governmental CERTs (EU: 24 of 28, NATO: 23 of 26).[7] NATO and the EU have an important role to play in establishing a Coordinating CERT that can support both governmental CERTs and national CERTs in member states.

4.2. Continuing Challenges for CERTs

The trends discussed previously challenge Servicing CERTs’ ability to operate as a reliable support group. Some of the most significant challenges are:

- **Budgets** – In today’s financially austere situation, the heavy workload can easily overwhelm the team. CERTs must find additional help outside their team, for example, at Product CERTs or specialized commercial Servicing CERTs.

- **Changing technological environment** – Also exacerbated by budget pressure, a CERT’s innovative ability to keep up with adversaries’ fast-evolving technological capabilities is being contested.

- **Skill levels of staff and retention** – Retention of qualified experts is also being challenged, mostly because the high demand for such specialized skills offers interesting opportunities outside CERTs. Maintaining the skill level of the current CERT’s members is also ever more challenging, due to the increasing diversity of devices in the ICT infrastructure and the increasing sophistication of incidents.

- **Information sharing, accuracy, and proprietary risks** – A main challenge for Coordinating and Thematic CERTs is the increasing need to share cyber security-related information with a growing audience. This requires standardized and trustworthy approaches for information exchange (e.g. mechanisms, formats, and procedures). Although this may seem to be a relatively simple technical issue, there is the deeper lying, rather complex issue of trust. This leads to questions such as: ‘can and should all security related information be shared? Are all CERTs willing to share information? Can all partners be equally trusted?’ In some cases, CERTs are not allowed to share information because they may end up disclosing companies’ confidential information, which could put them in an unfavorable position (e.g. disclosing ISPs’ weak levels of security performance), or cause them to breach privacy rules (e.g. ISPs information sharing with law enforcement agencies).

- **Clarity in coordinated action responses** – Coordination of action is another big challenge for Coordinating CERTs. The area of operation and the mandate of a Coordinating CERT are not always clear because of the complexity of the stakeholder network and the growing number of stakeholders. This creates significant operational risks.
Uniqueness of some responses by product, region, sector, or state – For a Product CERT, the challenges are in part comparable to those of a Servicing CERT. The benefit of a Product CERT is that it can focus on a (family) of product(s) or a single technology. The disadvantage is that it will have a more diverse customer base to serve. The workload of a Product CERT will most likely increase due to the demands of Servicing CERTs for external specialists. However, since Product CERTs provide commercial services, budget issues are less applicable in a growing market.

4.3. Next Steps

In order to overcome these challenges, CERTs would need to focus increasingly on a more specialized service portfolio, driven by their objectives and constituencies, and the urgency of the services they need to provide.

• Focus on a ‘First-Aid’ CERT – This type of in-house Servicing CERT would focus more on services that mitigate the possibility of a cyber incident and those that provide ‘first aid’ in case of a cyber emergency, typically driven by objectives like Detection, Containment, and ICT resilience.

• Outsource analysis and repair – Analysis and repair services could be outsourced and conducted by specialized and trustworthy cyber security service providers like Product CERTs.

• Outsource information gathering – Information gathering services could also be outsourced, typically to Coordinating or Thematic CERTs. By focusing on a smaller set of objectives, an in-house Servicing CERT can dedicate its resources to more advanced functions, such as predictive detection and dynamic repair.

• Improve internal security for device and patch management – In-house CERTs should reinforce their proactive services by improving their security tools (e.g. for secure device management) and executing patch management in a timely fashion.

• Improve in-house risk analysis, product certification tools, and monitoring – In-house Servicing CERTs should conduct risk analyses and product certification tests to continue developing a more resilient ICT infrastructure.

• Emphasize information and event sharing with other CERTs in the sector and the region – Information sharing within a collaborating network of CERTs should remain an important task for in-house Servicing CERTs. In some organizations, the units that conduct the more internally focused operational tasks are called Information Security Operations Centers (ISOC) or Computer Incident Response Teams (CIRT). As a result of the smaller services portfolio, the resource requirements can become more relaxed.

• Emphasize information and skill sharing with whole supply chain – Detection and containment services will require highly skilled staffs to be continually informed on ICT infrastructure’s threats and vulnerabilities and current detection technologies. The size of the staff could, however, be reduced from that needed for a full service portfolio. Part of the available budget could and should be invested in developing trustworthy agreements
and liaisons with suppliers. The need for specialized technical support can in part be fulfilled by external relationships with more highly skilled CERTs, such as Product CERTs. Since they focus on their proprietary products and technologies, such CERTs will not be able to handle incidents in their customers’ ICT infrastructures in a holistic manner. This need may over time give rise to outsourced Servicing CERTs that support in-house CERTs according to a contractually agreed service level. Such commercial Servicing CERTs would be incentivized to maintain a high level of technical expertise. However, they would need to invest in gathering information about their customers’ specific ICT infrastructure and architecture, and make arrangements to ensure that this knowledge remains confidential and current.

- Prepare for diversifying CERT landscape – Some CERTs should specialize on a smaller set of objectives, such as Identification and Business Continuity. CERTs may assume a coordinating role and concentrate less on hands-on services (like the coordination of handling individual incident in an organization). In that case, it would act on a higher level of coordination by maintaining a network of CERTs and other cyber security related parties, where responsibilities and mandates for action are well defined. An important element of such a network will be the level of trust in sharing information, primarily to enable members in the network to be more proactive. Another important element will be support for business continuity by mediating arrangements for disaster recovery. Ideally, this CERT will offer cross-domain consultancy, sharing lessons learned and guidelines for Responsible Disclosure.

The evolution of the CERT landscape will include non-profit and for profit firms providing awareness building, education, and training. Coordinating CERTs could provide these services in cooperation with their networks; however, it is more likely that they will be provided by commercial companies specialized in education and training. Some Thematic CERTs already exist as specialized CERTs with a focus on a specific business or technology theme. It is expected that more of these CERTs will emerge, like the Abuse Information Exchange between ISPs in The Netherlands, or the Anti-Phishing Working Group (APWG) in the United States, or the Info Sharing and Analysis Centers (e.g. the European FI-ISAC). The greater number of such CERTs will emphasize the need for trustworthy information exchange, as well as the need for coordination networks of CERTs and the likes.

Product CERTs can be seen as a form of specialized Servicing CERTs. It is expected that more vendors will establish some sort of Product CERTs, thereby highlighting again the need for trustworthy information exchange and coordination.

Refinement of CERTs’ service portfolios will encourage an increased need for collaboration and information sharing among CERTs. This will require organizations to establish relationships with various trustworthy partners. A Coordinating CERT (e.g. a National CERT) could play an important role in promoting, establishing, and maintaining such relationships.

5. Trust, the Key Factor

Information sharing, outsourcing, product certification, training, and all other types of collaboration in the cyber security realm must be bolstered by mutual trust. Several
studies, including Capgemini’s own research,[8] show that if there is no or insufficient trust between participants, there will be little chance for successful collaborations.

5.1. From People to Organizations

In the early phases of a CERT, relationships among individuals create a network of trust. The existing informal networks between CERTs have demonstrated to be very effective and should not be abandoned, even when CERTs evolve and the workload increases. However, from a managerial perspective, it is not reasonable or prudent to assume or even expect trusted partners to be able to offer help 24/7, for 365 days a year. Therefore, at some point, trust held in people needs to be transferred to organizations as the more dependable, yet more anonymous entities. Replacing individuals with organizations is a delicate process, where several aspects need to be taken into account.

When establishing trusted information sharing relationships, a CERT should consider its objectives and constituency in order to identify and limit both the information that can and should be shared and the audience with whom to share it. In fact, communities of interest (COIs) can be set up around specific themes. This is typically how some of the Thematic CERTs were created. When sharing information, all participants must accept the mechanisms of mutual sharing (e.g. ‘quid pro quo’ is a long standing principle in the Intel domain) and act accordingly.

As a result of Multinational Experiment 7 (MNE7), an Information Sharing Framework (ISF) for Collaborative Cyber Situational Awareness (CCSA) is being developed and implemented by the Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA)—a new organization involving governments, industry, and the military.[9] This is a very promising development since this framework has gained broad support from entities like European Network, the Information Security Agency (ENISA), the Department of Homeland Security (US DHS), and the Internet Engineering Task Force (IETF).

When establishing trusted collaborations, CERTs and their constituencies should consider a set of critical conditions:

- Parties should convincingly demonstrate a strict policy of integrity concerning each other’s confidential information. This calls for mechanisms like compartmentalization of information.
- Parties should, pre-crisis, agree on a service level describing how to respond to incidents. This may vary from providing advice only, to making active changes to the customer’s ICT infrastructure. Although in a commercial context the incentive for providing the services is money, the agreement must allow for action when required, and for a financial settlement after the fact.
- The service provider should be very transparent in its actions. The customer should be able to review and inspect the facilities at any time.
- The service provider should maintain a permanent staff, dedicated to specific customers. The staff should demonstrate a high level of skills and knowledge, with a proven track record.
- The service provider should deliver quality results. Such results should not only focus on handling incidents, but they should also include proactive measures. Action reports should include remedial actions, and show successes in protecting customers’ ICT infrastructure.
Trust is slowly gained, but can be quickly lost. In any collaboration, there will be moments of misunderstanding, below par performance, or expectations otherwise unmet. There is no prescription for what is acceptable and when the line, when crossed, is crossed irreversibly. The key is to maintain an open communication and act on facts. When sharing information or collaborating to counter security incidents, parties need to rely on the fact that behind the formalism of an organization there is still an individual responsible for the functions carried out.

5.2. Need for Enforceable Agreements and Trust-Reinforcing Institutions

In societies, organizations use contracts and formal agreements between them to create a mutually acceptable and defined level of trust. These agreements clarify the mutual obligations for the (bilateral or multilateral) parties involved. They also provide a means of pressure for settling affairs after the fact, if obligations are not honored as agreed.

While sound legal arrangements may be attainable at a national level, they are also necessary at the more challenging international level, where Internet borders have yet to be established. Supra-national organizations can and should play a vital role in solving legal arrangements issues.

Another mechanism for building trust between entities is obtaining the endorsement of a neutral organization that aims at building trust between parties in the cyber security domain, like the Forum of Incident Response and Security Teams (FIRST) and Trusted Introducer (TI). The endorsement of these organizations (e.g. certification at different levels) presents an objective assessment against pre-set criteria of the way CERTs handle information and security incidents, and protect themselves against security incidents.

5.3. Reinforce Professional Ethics

Despite all the recommended measures described above, services are ultimately delivered by people, or at least performed under the responsibility of people. Legal arrangements and technical measures are important between organizations, but they can never fully replace the ethics of individuals. Perhaps, it would be useful to introduce a form of ‘Hippocratic oath’ for cyber security experts, such as: ‘I swear that I shall always try to the best of my ability to maintain the health of the ICT infrastructure that has been entrusted to me and always share my cyber security knowledge with my fellow oath-takers for free.’

Recommendations and Conclusions

Organizations are becoming more and more vulnerable to cyber security incidents, due to their increasing dependency and complexity of their ICT infrastructures and connectivity to other parties.

At the same time, cyber incidents are growing in scope, sophistication, and frequency. These trends and the inherent nature of the borderless Internet call for the urgent creation of national and governmental CERTs to be part of the EU and NATO member states’ network of CERTs, if they do not yet exist.
The trends result also in a growing workload for existing CERTs, thus calling for better responsiveness and more adaptability. CERTs can only meet these challenges if they focus on a smaller portfolio of more advanced services, while being able to depend more and more on trusted partners for services they cannot provide themselves, and reliable sharing of security related information.

Trust is the key factor for successful collaborations and information sharing in the cyber security domain. Trust must be built carefully, at first between individuals and later between organizations. Active measures must be taken to establish a network of trusted partners and foster each individual relationship. Independent third parties can play an important role in this task. The cornerstone in any relationship will remain trust between people.

References

[7] Ibid.