GvIB Expert Letter – March 2006
ISSN 1872-4884, Volume 1 – No. 1

CERT in the organisation

Ron Tolido

Patrick Borsoi

Henk Bronk

Ben Elsinga

Rob Greuter

Wim Hafkamp

Aart Jochem

Martijn van der Heide

Kelvin Rorive

Thom Schiltmans

Jacques Schuurman

Roeland Reijers

This Expert Letter deals with the increasingly important phenomenon of in-house Computer Emergency Response Teams (CERTs). The number of internal CERTs in larger, commercial organisations has increased rapidly in the past few years. This is mainly in response to the painful security incidents that have taken place during the past few years on Internet and which have been observed in the minutest detail by millions. Issues concerning necessary competencies, procedures to be followed, the availability and the tools to be used affix themselves to CERT within an organisation. But the greatest challenge appears to lie in the relationship with the existing IT organisation, both in terms of division of tasks and responsibilities and mandate. The ultimate question to be answered is that of the life cycle: will CERTs always be needed or will they eventually be absorbed by the existing IT organisation. In other words: will CERT ultimately make itself redundant?

http://www.gvib.nl/

expertbrief@gvib.nl

1. BACKGROUND

During the past few years, the number of internal Computer Emergency Response Teams (CERTs) in larger, often commercially operating organisations has greatly increased. The first CERT dates from 1988. It was established in response to a so-called *malicious code* incident. The Morris 'worm programme', named after its infamous creator, then knocked out 10 percent of computers connected to Internet worldwide. Even with the more limited scale of Internet at that time, the consequences were startling. The security incident led in the U.S. to the establishment of the CERT© Coordination Center (CERT/CC) by the Defense Advanced Research Projects Agency (DARPA).
A few years later, in 1991, the decision was taken during a SURFnet customer contact day to establish the first official Dutch computer emergency response team, CERT-NL, a CERT for customers and users of SURFnet.

The term CERT is a registered trademark of the CERT/CC of the Carnegie Mellon University. See the website www.cert.org for more information if you contemplate using the term 'CERT' for commercial or non-commercial purposes.

The emergence of in-house CERTs can be traced back directly to the increasing number of Internet-related security-incidents during the past few years and thus – potentially – the increasing likelihood of substantial trading loss. The incidents, mainly *spam*, *malicious code* and *hacking*, require an immediate, coordinated response by well-trained specialists. Since an ever increasing claim is made on the existing IT management organisation, many organisations choose to establish separate teams for this: The teams mainly consist of very specialised IT experts, who focus on subjects like *operating systems*, *network protocols* and *vulnerability management tools*.

Each CERT works for a so-called *constituency.* In most cases, organisation's own business and IT departments are involved. In the case of (IT) service providers, the customer groups sometimes belong to the constituency but, in the context of this expert letter, we regard this as an exception.

The design of a CERT is not an easy matter. The first challenge is finding and holding on to professional, motivated staff. The CERT must also continually render added value, especially in relation to the necessary investments in people, equipment and accommodation. It also has to operate in a difficult field of tension, which also shifts over time, with the IT management organisation(s) and the buyers of IT services.

2. RESEARCH QUESTIONS

The main question that the Expert Letter study group originally asks is one with a high prosaic content.
How is a CERT effectively and efficiently established within an organisation?

To answer this question properly, the following subjects must at least be covered:
1. What are the main and subsidiary tasks of the CERT?
2. What is the desired quality and scope of the CERT when services are provided 24 hours a day, 7 days a week (number of FTEs, educational level, experience, consignment timetable, etc.)?
3. Which procedures does the CERT employ (Operational Framework)?
4. Which tools does the CERT use?
5. Where is the CERT positioned in the organisation?
6. Which mandate/competencies does the CERT have (and which does it NOT have)?
7. What are the relationships between the CERT activities and the ITIL management organisation (in particular with Incident Management, BCM, Change Management and Security Management)?

During the work session it becomes clear that the first four questions can be relatively easily addressed: there are many useful sources available and there is an increasing level of standardisation. Striking in this respect is that the design and functioning of a CERT is often regarded as problematic in practice: why is this so difficult, while there is already so much known?

The last three questions – which all concern the relationship of the CERT with the existing organisation – give rise to a fundamental discussion about the life-cycle of a CERT. The special character of a CERT (after all directed towards responding to unpredictable events and handling crises) ensures that the team will often occupy a distinct position in the organisation in the early phases of its existence. However, as the CERT becomes more closely interwoven with the existing structures and processes, the separate status becomes increasingly less desirable. Frequent testing of the team's own functioning and the positioning within the organisation is therefore essential. This leads to an interesting, existential follow-up question:

What is the life-cycle of an in-house CERT?

Once the purpose and the position of an in-house CERT comes up for discussion, there is no harm setting sights on possible (cheaper) alternatives. The *UK National Infrastructure Security Coordination Centre* (NISCC), for example, recommends the implementation of a *Warning, Advice and Reporting Point* (WARP). With the aid of a specially designed toolbox, this supplies all kinds of services and products that are related to those of a CERT. It appears that there are also organisations that have effectively prepared themselves for security incidents without the establishment of a separate CERT within the organisation.

4

3. TASKS AND ROLES: GOOD DEFINITIONS AVAILABLE

A Computer Emergency Response Team (CERT) is a team that responds to IT-related security incidents by offering services with which incidents are solved or which contribute to the solution. Steps are also taken, in accordance with the assigned responsibilities, to prevent security incidents within the user constituency belonging to the CERT.
The primary focus of a CERT therefore lies on responding effectively to security incidents that are associated with IT and that possibly have an impact on the constituency. The secondary focus on preventative activities – for example, advising on weak spots in systems and on the danger of viruses – should ensure that potential risks are limited and that the CERT has to come into action as little as possible.
The following, mutually comparable terms are also used to indicate a CERT:

- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- IRC (Incident Response Capability)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)
- SIRT (Security Incident Response Team)

Types of CERTs

Besides the type of CERT which this expert letter focuses on – an in-house CERT – other types of CERTs can also be distinguished. A selection:

- Small & Medium Enterprises CERT
  - This is a CERT that has several small and medium-sized businesses in its constituency, usually because the companies in question are themselves too small to establish their own team.
- Academic CERT
  - This is a CERT that focuses on the constituency of universities, colleges, laboratories and research institutes. The CERT phenomenon has for some time been mainly associated with the academic world, not in the least because Internet came into its own in this context.
- Military CERT
  - A CERT that focuses on the constituency within the defence world, including affiliated administrative institutes.
- Commercial CERT
  - Commercial CERTs offer their specialised services to every company that for whatever reason does not want or cannot establish their own CERT.

Standards for design and management

Over the years, a lot of experience has been gained with the design and management of CERTs. Exhaustive, very comprehensive standards have been published that focus on the range of duties, the roles, the organisational interpretation and the tools to be used.

GOVCERT.NL, the CERT for the Dutch government has even published a 'CERT-in-a-box': a CD containing all information, checklists and tools that are required to design a CERT.

Crucial for every organisation that gets involved in the CERT phenomenon is Request For Comments (RFC) 2350 from the Internet Engineering Task Force (IETF). The IETF is a large, international operating network of interested parties concerned with the architecture of Internet and its smooth operation. RFC 2350 was already published in 1998 and should function as a basis for the design of every CERT: it provides guidelines for the description of services, constituencies, procedures, expectations, etc. RFC 2350 is acknowledged to such an extent that there are even some accreditation models based on this document: organisations can have their CERT formally certified with RFC 2350 in hand. With all this it is clear that organisations wanting to establish their own in-house CERT can best follow the RFC 2350 template. Broadly speaking, this comprises the following elements:

- Contact information
  - Names, addresses, telephone numbers, email, etc.
- Charter
  - Describes the mission of the CERT, the constituency, the way in which the sponsorship of the team is arranged and the assigned mandate
- Policies
  - Description of the types of incidents requiring a response, the level of support to be provided and the policies to be followed regarding communication, cooperation and interactions, both within and outside the organisation
- Services
  - More detailed description of the services to be provided in the context of the response to security incidents, in terms of addressing and analysing the incident, coordinating the required tasks, and the actual resolution of the problem. Preventive services are also included under this heading.
- Documentation
  - Summary of electronic and manual procedures for reporting and documenting incidents.

4. GETTING IT RIGHT FROM THE START

Given that CERTs have now been used for about 18 years, a wealth of knowledge and experience is now available regarding the establishment and operation of these teams. Yet establishing and running a successful CERT in practice is still a difficult challenge. From this past experience it is however possible to formulate some 'best practices' of potential benefit to any CERT operation:

Listen to your target group: define a USP for your CERT

While CERTs often tend to operate in isolation because of their highly specialised expertise, it is essential to keep talking to the community of users that gave rise to the project in the first place. Following an excessively mechanical approach simply based on "ticking the boxes" can easily lead to subtleties in the requirements of your constituency being missed. And that in turn can be the difference between success and failure, particularly in terms of success as perceived by the user community.

So it is important to be attentive to the wishes and needs of your user community. Always remember that the requirements can vary widely from one organisation to the next. for example, a CERT working at a university will be dealing with a target group that provide some very specific challenges. The "user community" here will be made up of intelligent and 'switched-on' young men (or indeed women) who are often totally *au fait* with the latest advances and techniques. So it is no surprise that the relatively new phenomenon of 'phishing' has been well-known for several years in this particular environment.

Each CERT should formulate a 'unique selling point' (USP) for its organisation, a 'raison d'être' that is so precisely tailored to the mission and characteristics of the organisation as to be immediately recognised across the entire structure. This kind of USP will help the CERT to be adopted and properly acknowledged by its organisation, and will also give the team the extra momentum required for its successful establishment and operation. A CERT that is not able to formulate a convincing USP should ask itself whether there is any point in having a team, and its view of its own organisation. Particularly now, when it is almost seen as being 'hip' (or even 'cool') to set up a CERT, or to be part of one, it is essential right at the outset to ask the fundamental question of whether there is any need for a CERT in the first place.

Ideally, the managers in charge of the business should be asked to draw up the CERT's mission statement themselves. This is the best way to ensure that the goals set for the team will be real ones, and to guarantee buy-in and recognition from the organisation. As well as focusing the process in the right direction, drafting the mission statement jointly also helps to set the top priorities, so the CERT gets a clear picture of the steps that need to be taken first.

Be flexible

A successful CERT has to place considerable weight on defining and following standard procedures. But flexibility is even more important, because, by definition, its area of work includes unexpected crises that are difficult to foresee: fixed procedures will only be effective for 70% of all incidents occurring, at best. 'Inflexibility' and 'CERT' should be mutually exclusive concepts.

Being flexible also means that the CERT must always be ready to work beyond company boundaries: that is where potential crises start, and also where the knowledge and skills needed to deal with the problem can be found. One of the reasons for the failure or ineffective operation of some CERTs, even after 18 years, is an inability to share knowledge effectively, both within an organisation and more particularly between organisations.

One of the major challenges is often in the gulf between the adaptability required of a CERT and the much more rigid character of management organisations. Collisions can easily occur.

Find the optimum place within the organisation

Organisation theory teaches us that there is no one ideal way to set up an organisation. And even if there was, it would rapidly become outmoded. The constraints are constantly shifting, and 'successes achieved in the past are no guarantee for the future'. Accordingly there are a range of 'best practices' regarding the place of a CERT within the organisation, depending on factors such as the organisation's size, the maturity and experience of the local IT departments, the extent to which they are embedded in the operation of the company, the management style, and the ways in which the impact of a disruption can be detected, locally or otherwise.

Particularly for a large organisation with distributed structures, a central CERT will probably be indispensable. But given the all-important relationship with the user community, it is vital to be as close as possible to the 'shop floor', since that is where the real impact of potential crises will be felt. On the one hand you have to be able to work fast and effectively, and on the other you need to be able to exert real influence - where applicable - over the management of the organisation.

There are known cases of successful CERT structures in which each business unit has its own 'CERT light', coordinated by one overarching CERT. This sort of coordinating entity is be essential for such a structure, if only to ensure the required sharing of knowledge.

In contrast, some relatively large organisations prefer to have one central CERT, with smaller 'CERTs light' within each IT department (as opposed to business unit). In that situation it will be important to consider the extent to which a local incident management function is already present in the IT departments. This again involves the interesting issue of the appropriate relationship between the CERT and IT structures.

Another alternative cited is a true network structure, comprising several independently operating CERTs (closely associated within or actually within the respective business units), structured as a loose matrix.

Sometimes the best option is to create a 'virtual team'. Rather than being set up as an organisational entity in its own right, the team comprises representatives of other units. This option is likely to be appropriate where there are obstacles or issues around making changes to the organisational structure. This can also be a viable strategy for anchoring the team better in the management structure.

In the current environment, with more and more (IT) activities being outsourced, it comes as little surprise that some organisations choose to outsource some of the tasks of a CERT to an external provider. The role of the external specialist provider is then often to raise the alarm

in the event of impending or actual security incidents. A small internal team is then tasked with arranging the required internal communication processes and coordinating the activities of the IT departments. Not infrequently, the IT departments' role is also outsourced. Hence the effective *management* of all the parties involved – wherever they are located – becomes an art in itself, and the issues around the mandate become even more evident.

RFC 2350 sets out the tasks and relationships of a CERT in great detail, but the document says nothing about how the team should be embedded in the organisational structure. The working group considers that this may well prompt the development of *organisational 'patterns'*, and believes that these, in combination with a description of characteristic environmental factors, may provide the basis for decisions to be made around the issue of integration within the organisation. This topic is clearly too specialised to be addressed in this Expert Letter, but could possibly be examined in a follow-up session. It would also be a worthwhile topic for a final year elective in the academic environment.

Grow an environment of trust

Trust is an essential foundation for the satisfactory ongoing operation of any CERT. That means getting a mandate from all parts of the organisation, including top management, not as a matter of entitlement, but by earning their confidence in the team's practical contribution.

All parties - both within and outside the team - must be absolutely clear on when the CERT is to become involved, and the authority levels that it then has. The situation could be compared to pulling the emergency cord or ringing the fire brigade: this is something you do only for very good reason. Getting it wrong can be very expensive - and once the CERT has been activated on the basis of a false alarm (resulting in all the company's computer systems being shut down for a few hours for security), it will probably be much harder to convince the organisation of the need for their intervention next time. 'Severe penalties' really do apply, and it is therefore essential to keep a cool head in an environment sometimes characterised by over-hysterical reactions to a possible disruption.

The ultimate decision on whether or not to 'pull out the plug' is, and remains, a business decision. If the systems of a railway company are shut down, for example, some 100,000 commuters could be stranded at the country's railway stations. In this kind of situation it is absolutely crucial to have access to accurate information, and even more important that there is a relationship of trust between everyone involved, through all parts of the organisation. Only if the CERT is able to operate in a 'trust ecosystem' that it has created and nurtured can it be said to have a 'mandate' in the true sense.

For practical reasons, ultimate authority to 'pull the plug' will often lie within the operational management structure. In the case of serious, genuinely acute threats there will always be too little time for careful consideration of the matter at management level. *Shoot first, ask questions afterwards*, then inevitably becomes the rule.

Current technology does, however, help to assess the impact of a possible disruption more accurately, particularly in comparison with the situation 18 years ago. Extensive standardisation and business intelligence tools (e.g. Open View from HP and Tivoli from IBM) enable a CERT to translate the impacts of problems in the infrastructure directly into the operational consequences, down to the level of specific processes, business units and even customer relationships. Within state-of-the-art management environments of this type, 'business process views' can instantly identify the impacts of an incident (or potential incident) at the level of business processes. For example, one European telecom company has used a 'cashflow assurance system' to quantify the impacts of an incident on its core business operations.

But even in these situations, far more important than even the most detailed pie chart is mutual trust. Ultimately we are working with people, and as the working group has stated so trenchantly, 'sometimes the best form of lubrication is a glass of beer'.

5. RELATIONSHIP WITH THE IT ORGANISATION

The question of the relationship between the IT department(s) and the CERT is related to the broader issue of the team's integration into the overall organisational structure. A good relationship with the IT structure is crucial for the success of a CERT, as is the relationship with management. The issues involved relate to mandate, flexibility, sharing of knowledge and the maturity of processes. Here again, the location within the organisational structure depends by definition on the individual situation, and over time the solution adopted will tend to become less viable and effective.

In many cases the CERT is simply part of the IT structure, if only to ensure that the required action will in fact be taken immediately ('otherwise you could imagine a situation where the CERT said "thou shalt not patch", but the IT department, based on ITIL, did just that'). Often, however, an explicit decision is made to keep the two environments separate. Part of the reason for this lies in the inherent difference in dynamics: a CERT has to be able to take prompt and decisive action, whereas an IT department – possibly standardised on ITIL – is likely to put the emphasis on predictability and repeatability. The ability to react to unexpected incidents is a distinct speciality, which may well extent over several different platforms, organisational entities and stakeholders. In addition, a CERT's operational focus is generally on resolving sudden crises, whereas the IT department is typically more concerned with ongoing security management, incident management and change management functions.

Yet by definition there is considerable overlap between the two areas of work, and each may impact on the other. Particularly when the question of the *mandate* arises ('when that plug has to be pulled, out it comes'), this can prompt a clearer definition of processes and interfaces. So on the establishment of a CERT there can be a rebound effect generating a leap forward in the level of maturity of the IT department. Even the debate on the demarcation between 'incident-related' and ongoing issues can give rise to the implementation of improvement suggestions in the IT department; issues that necessarily have to be addressed in the first instance by the CERT later tend to become part of the permanent IT structure.

This insight points the way to an important conclusion: an effective CERT can only thrive in combination with a truly mature IT department - and many IT departments have not yet attained that level of maturity. This only becomes evident when a CERT is set up. An improvement process should be the logical consequence, so that over time, the position and operation of the CERT should evolve towards its original mission: to respond to unexpected security crises.

According to the level of maturity and other environmental factors, an 'incident response' structure can also take many other forms. The *UK National Infrastructure Security Coordination Centre* (NISCC), for example, recommends the implementation of a WARP (*Warning, Advice and Reporting Point*). Under this arrangement, a specially developed toolbox is used to deliver all the services and products related to those of a CERT. The centre would, however, have more of a coordinating and knowledge-sharing role, as opposed to the operational focus expected of a CERT. Operational aspects are seen as being integrated as mature functions in the IT structure. 'ISA' centres operate in a similar way. These centres are mainly focused on the gathering and dissemination of information, given that in practice this is one of the success factors for a rapid response to new disruptions.

Indeed, there appear to be plenty of organisations – in the Netherlands as elsewhere - that have made perfectly effective preparation for a security incident without setting up a separate CERT within their structure for this purpose. So clearly a level of maturity has been reached within their IT departments that effectively combines standardisation and repeatability with the flexibility required in order to deal with sudden security crises.

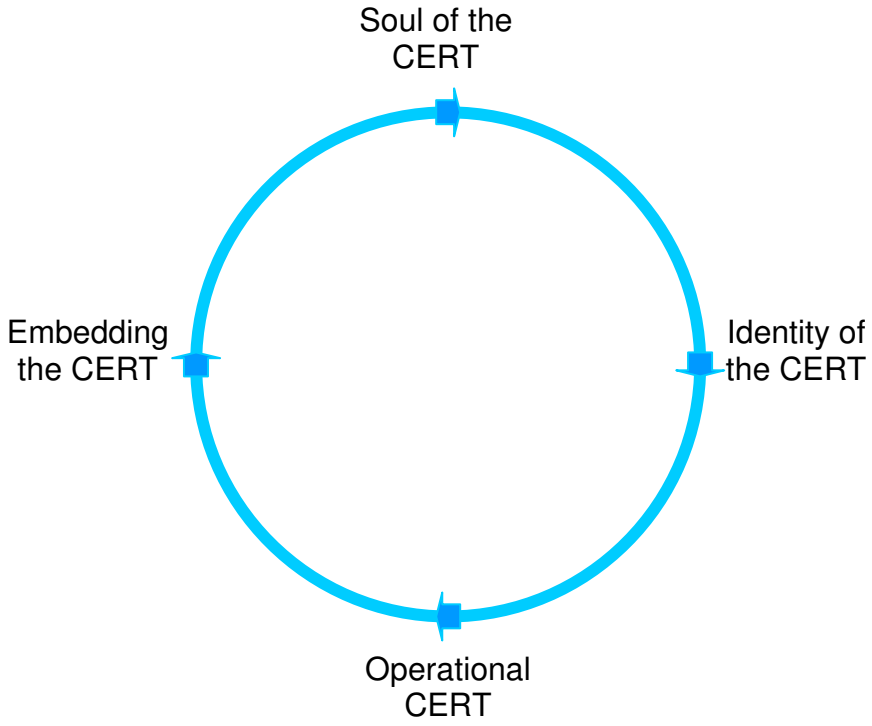
Remember that in all cases it is the local situation that determines the priorities for the measures to be implemented, because the requirements for timeliness, speed and effectiveness will vary according to the situation.

6. LIFE CYCLE OF A CERT

A CERT can be seen as one of cogs in a complex system of internal and external circumstances, or even as part of an 'ecosystem'. Such a system never stops, and as stated earlier, no perfect state is ever reached where nothing more needs to be changed.

So it is only logical to see every CERT has having an individual, self-calibrating 'life cycle'. When the cycle has been completed, this may prompt changes to the mission, generating another full or partial cycle to be completed. Hence the number of cycle iterations is potentially infinite, because the ecosystem is constantly changing and evolving.

The life cycle has 4 clear stages:



Stage 1: **Establishing why the organisation needs a CERT**. This is the creation of the CERT's 'soul'. The CERT will never be successful without a soul, so this stage is crucial for its ultimate performance. The first step is to give careful consideration to the mission and organisational environment and the linkages between possible disruptions and the operation of the organisation. Generally speaking, if it is to recognise the 'soul' of the CERT, the organisation must have been involved from the outset in drawing up its mission and tasks. A business case for the CERT will help to place the required investments and efforts in their correct perspective.

Stage 2: **Completing the CERT identity document**. This is best carried on the basis of the very comprehensive RFC 2350 document. The identity document is the 'birth certificate' or charter with respect to the permanent organisational structure. Fortunately, CERTs do not have to 'reinvent the wheel', and in these days of 'CERT-in-a-box', predefined templates and the first drawings of 'patterns', this stage will take less time than you might think.

Stage 3: **The actual performance of the required activities**: The CERT is now fully operational, performing a mix of proactive and reactive activities.

Stage 4: **Embedding the CERT in the organisational structure.** This is an adaptive process, where the creation and fine-tuning of standards, guidelines and processes go hand in hand with growing the crucial environment of mutual trust. This is actually a transformation process, in which all the parties involved learn and change to a greater or lesser extent.

As stated earlier, when this cycle has been completed it will often be necessary to test whether the environmental factors are still the same. Changes can occur both within and outside the organisation, and as already noted, setting up and running a truly effective CERT can also have direct impacts on the maturity of the organisations IT departments. The 'soul' of the CERT may sometimes change in the course of time, along with the appropriate way to anchor the team in the organisational structure. This can give rise to a different 'identity document', which in turn determines the form of the new iteration of the remaining life cycle stages.

The use of the 'life cycle' concept is a deliberate choice on the part of the working group: the point we are making is that each stage must be completed in the correct sequence. A CERT that goes straight to stage 3 activities has no chance of succeeding. Yet this is precisely what often happens, driven not least by current trends and the crazy times we live in, and this is largely why now, 18 years down the track, the establishment and maintenance of a CERT is still no easy undertaking. From the above it also follows that a CERT may be perfectly functional now, but will not remain so indefinitely. This could only be the case if the rest of the world stayed the same, and there would appear to be little chance of that happening.

7. A CERT'S ULTIMATE GOAL: TO BECOME SUPERFLUOUS?

Having this lofty level of self-reflection, there is one final question to be answered: is there perhaps a *stage 5*, where the CERT has made itself superfluous, so that it can then be abolished? And if so, will the convinced, fanatical CERT member quietly accept this new reality, without opposition (at least on an unconscious level)?

One thing is certain: in a genuinely mature IT structure, where standardisation and repeatability go hand in hand with flexibility and adaptability, a CERT will always have less to do than might initially be expected. Our working group believes that a CERT working under pressure with an overfilled whiteboard of 'to do's' is generally a sign of a dysfunctional, or at least immature, IT structure (as confirmed by management theory: really efficient managers generally have lots of empty space in their diaries).

So it should generally be possible to abolish a CERT once all the required functions and activities can be carried out successfully by the permanent organisation. Another possibility is the outsourcing of all crucial processes to an external service provider, so there is simply no further need for an in-house CERT. Changing external and internal circumstances can also reduce the scope to the point where the business case for a separate CERT no longer stands up.

8. CONCLUSION

Our working group believes that enough issues of interest remain for coverage in a future Expert Letter. These include the following: 'patterns' for embedding the team in the organisational structure; the use of advanced business intelligence for a more accurate view of the impact of disruptions; and the issue of whether over the many years of CERTs based on standards such as RFC 2350, there may have been so many changes (e.g. the proliferation of laws and regulations, open source, transparency, growth in the scale of the Internet) as to justify a reassessment of the applicable standards.

However that may be, we have noted that the ongoing completion of the CERT life cycle, including retesting of the mission and 'soul' of CERT teams, will automatically show when a CERT has become superfluous or - better still - has actually done itself out of a job. If this final stage causes some pain for those involved in the CERT in question, that is only to be expected - we are only human. On the other hand, a simple Buddhist aphorism teaches us that pain is caused by clinging to the illusion of stability in a world where everything must always change. Which is probably the perfect way to end this Expert Brief.

We wish to express our thanks to ***Ton van Gessel*** for his valuable assistance with preparations for the Expert Letter session.

We would also like to thank the company **KPMG** (www.kpmg.nl) for sponsoring the translation of this paper from Dutch to English.

If you like this paper or if you have important remarks, please send an e-mail to expertbrief@gvib.nl

16

LITERATURE

The following literature was consulted by the working group during the preparation of this Expert Letter on CERTs in an organisation:

[1] Patrick Borsoi, *CERT-functionaliteit bij een grote overheidsorganisatie*, juli 2005

[2] Chris Alberts e.a., *Defining Incident Management Processes for CSIRTS: a work in progress,* oktober 2000

[3] Moira West-Brown, *Avoiding the Trial-by-Fire Approach to Security Incidents*, Crosstalk oktober 2000

[4] Stanford White Paper, *International Coordination for Cyber Crime and Terrorism in the 21st Century Version 6*

[5] Bart Bokhorst en Jan Schapink*, PI-Studie Basisnormen Beveiliging en Beheer ICT-infrastructuur*, EDP Auditor 2003-4

[6] *Coatings team Incident Response Conclusions*, AKZO Nobel presentatie 17 september 2003

[7] *ISF SoGP - Incident Management,* Parts taken from the ISF Standard of Good Practice

[8] *CERT-in-a-box*, uitgave van GOVCERT.NL

[9] Kevin Rorive, *ITIL is een zegen voor Patch Management*, Informatiebeveiliging Jaarboek 2004/2005

[10] Moira J. West-Brown, *Handbook for Computer Security Incident ResponseTeams (CSIRTs),* CMU/SEI April 2003

[11] Linda Kelver, *Incident Response in A Global Environment*, GSEC Version 1.2b, SANS Institute 2000-2002

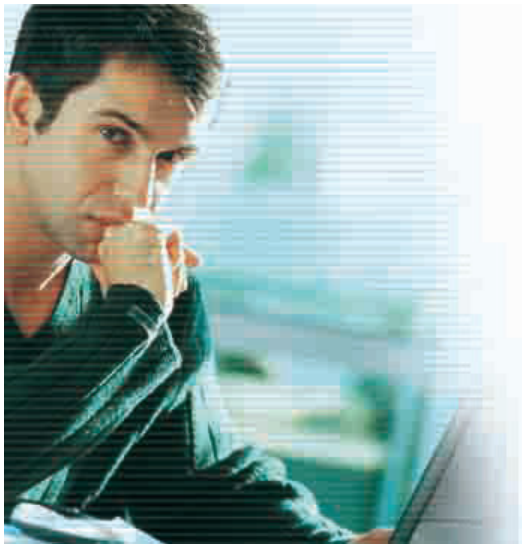
[12] N. Brownlee, E. Guttman, *Request for Comments (RFC) 2350*

APPENDIX: LICENSE FOR THIS PUBLICATION

This expert letter has been published according to the following license:
http://creativecommons.org/licenses/by-sa/2.5/

18

JOIN THE GVIB, FOR SAFETY AND SECURITY ...



Information security has been an essential and exciting subject for many years. Almost all occupations are having to place more emphasis on the confidentiality, availability and integrity of their information. Whether you are a CISO, manager, consultant or programmer, the Information Security Practitioners Association (GvIB) can help you with information security issues.

What is the Information Security Practitioners Association?
The GvIB is an open, broad-based association for professionals to build a more professional approach to information security, through the exchange of ideas, information, knowledge, insights and above all, practical experience.

What are our aims?
We aim to promote the physical, systems and organisational security of data and data processing equipment against in-coming and outgoing breaches. We also promote the exchange of knowledge and experience and the networking of practitioners in the sector - through this Expert Letter, for example.

Our target group
The target group for the GvIB includes everyone involved in information security, either as a student or professionally, or who are especially interested in the field. Our rapidly growing membership covers many different disciplines: students, information architects, technicians, managers, organisational consultants, legal specialists, security officials and ICT auditors. Our members come from all kinds of educational backgrounds, companies, public authorities, organisations and suppliers.