Effectiveness of Proactive CSIRT Services

Johannes Wiik *<Johannes.Wiik@hia.no>*
Jose J. Gonzalez *<Jose.J.Gonzalez@hia.no>*
Faculty of Engineering and Science
Security and Quality in Organizations
Agder University College – 4898 Grimstad, Norway

Klaus-Peter Kossakowski *<kpk@sei.cmu.edu>*
Software Engineering Institute in Europe – 60322 Frankfurt, Germany

Abstract

Many authors have suggested that Computer Security Incident Response Teams (CSIRTs) need to deliver more proactive services to stay effective, but there are hardly any studies investigating to what extent existing proactive services are indeed effective or how to make them more effective. Indeed the advisory service is one of the core CSIRT services and proactive in scope – already part of the description even in the oldest CERT related documents. Experiences show that the service itself has not changed much over the years. Only some technical development can be seen in regard to system categorization, identification schemes for vulnerabilities or formats for the effective exchange.

We view the proactive services as cross-organisational learning processes, where CSIRTs facilitate learning between information providers (i. e. vendors of commercial off-the-shelf-software) and users of these information (i. e. users of such products) in the CSIRT constituency. We evaluate and compare two proactive services:

1. The common advisory service as an example of an existing service, and
2. Neighbourhood watch (NBHW)[1] as a new service that builds on the advisory service.

Based on organisational learning theory, we made a conceptual system dynamics model to compare and discuss the effectiveness of the two services. We found that neighbourhood watch as a learning process significantly addresses several weaknesses in the traditional advisory service with respect to knowledge acquisition, information distribution, information interpretation and organisational memory.

Our conclusions support our argument that the potential of proactive services should be viewed as a cross-organisational learning process. They carry the promise of avoiding incidents and the hope of saving considerable resources, but only if the constituents are enabled to learn from the experiences of the past and from others effectively.

This last issue is important in order to put our observations back into the broader picture. It stresses again [Wiik et al. 2005a,b] that all CSIRT related activities are impacting each other and cannot be seen as separate activities. As current management approaches do not consider this aspect, we recommend to all CSIRTs to revisit their services and interdependencies not yet addressed in their current setup.

1 Developed by DFN-CERT, neighbourhood watch is one of their proactive approaches. NBHW is actively searching for vulnerabilities in networks and organizations. Quite specific information is provided through analysis of systems within the constituency and informing the administrators about much needed patches or changes to the setup. Rather than carrying out this analysis only on demand the networks and systems can be monitored routinely or ad-hoc, if some crisis is developing. Thus, it is similar to (and hence we call it) a "neighbourhood watch": your neighbours keep an eye on your assets. [Grabarske 2005]

From Reactive to Proactive Services

Despite the fact that CSIRTs have developed over almost two decades, there is still no widely accepted way to classify an organisation as a CSIRT. We will use the definition in the CSIRT handbook: "For a team to be considered a CSIRT, it must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination." [West-Brown et al. 2003, p.23] Given this definition, a CSIRT should therefore mainly be considered reactive in nature.

A simple way to describe a CSIRT's mission is: "to minimize the impact of an incident to a company and allow it to get back to work as quickly as possible" [van Wyk, Forno 2001], or "to be a focal point for preventing, receiving and responding to computer security incidents" [Killcrece et al. 2003b p.xi]. It is the responsibility of CSIRT managers to achieve such goals. There are many options and a wide range of services can be offered by a CSIRT to accomplish their goals. Some of the services target proactive prevention of incidents, while others minimise the negative consequences of incidents in a more reactive manner.

There has been a growing realisation that more proactive services are needed [Killcrece et al. 2003b, p. 112 and p. 131]. Traditionally the advisory service is the "blueprint" of any of these services as it was provided by CERT/CC since its foundation in 1988. In more recent years some CSIRTs have extended their service offerings and included new proactive services. However, a proactive measure to prevent all incidents from happening is not a likely strategy to succeed based on the assumptions in the survivability paradigm. Thus, the question is not whether we need reactive or proactive services, but rather how to find the right balance between the two. And maybe even more important, how to make proactive services more effective. As Bruce Schneier explains regarding proactive action [Schneier 2000, p. 374]: "We can do demonstrably better than we are, but everything we know about complex systems tells us that we cannot find and fix every vulnerability." Still there is much room for improvement.

The Goal of Proactive Services

Information technology products are vulnerable. Surprisingly, the majority of incidents exploit vulnerabilities where a solution, most often a patch, is already available [Arbaugh et al. 2000]. According to Egan and Mather, on average it takes 6 months from the disclosure of a vulnerability until it is exploited [Egan, Mather 2005, p. 200]. We would rather not argue on a specific time period here, as this time frame has been continuously declining, and all we can expect is that there will be even less room to manoeuvre in the future. As new vulnerabilities are continuously disclosed, a hardened system will inevitably oscillate between a vulnerable state when a vulnerability is disclosed, and a hardened state when a fix or a work around has been applied. In some cases they might also become compromised. The goal of course, is to avoid such incidents, and hence keep all systems in a hardened and uncompromised state.

The main catalyst for exploits is not the disclosure of a vulnerability nor is it the release of a patch. The catalyst comes when the exploit is automated (i.e. hacker tools that exploit the vulnerability are released on the internet). We can therefore summarise a typical life cycle of a single vulnerability in the following time graph [Arbaugh et al. 2000].

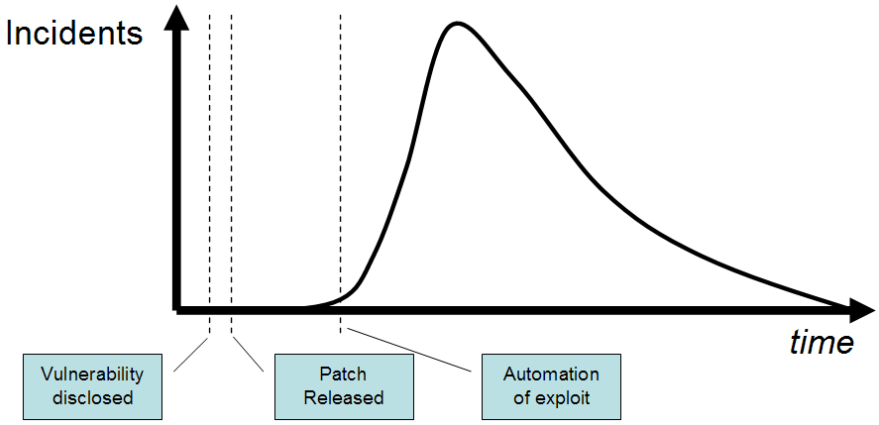

Figure 1: Incident rate in a single vulnerability life cycle according to the findings of [Arbaugh et al. 2000].

Overall automation of exploitation has two main effects:

1. More people even with limited knowledge are able to exploit the vulnerability
2. Automation increases the frequency by which attackers can exploit a vulnerability more widely.

The result is a quick rise in the number of exploits after its automation. Arbaugh also found evidence of a very long tail before the exploitation of the vulnerability was reduced significantly. In some cases this process took several years, indicating that numerous systems were vulnerable in this period. Possible explanations for the decline can be attributed to a surprisingly slow reaction from system administrators [Arbaugh et al. 2000, Wiik et al. 2004], or from the fact that offenders turn to other vulnerabilities [Lipson 2002]. In addition, reinstalling software can reintroduce an old vulnerability if the new full installation does not contain the patch. This also applies for backups or images which are used to speed up setup time.

Therefore the goal of any proactive service must be to provide the information about an existing vulnerability and available solutions before automation of an exploit takes place; that is, to allow mitigation efforts from all parties involved in order to bring as many systems into a hardened state as possible. As argued by us before, a CSIRT might help organisations to harden their vulnerable systems [Wiik et al. 2004]. For this to happen, a CSIRT has to help its constituency to learn. Indeed this is the purpose of the advisory service. Nevertheless there seems to be several barriers that need to be overcome for effective learning to take place. To understand these it is necessary to review what we know about organizational learning.

Organizational Learning and the Advisory Service

We might identify several learning processes related to incidents and their prevention that relates to CSIRTs and the environment around it. For example, learning can take place within the organisation experiencing the incident, vendors of vulnerable software or a CSIRT. Our main interest is how the CSIRT learns and to what extent organisations within their constituency learn from the CSIRT. In other words, learning has to take place across multiple organisational barriers.

According to Sagan, learning needs to take place across organisations, but he also acknowledges that current research has not provided any deep understanding of such cross-organisational learning [Sagan 2004, p.18]. A good way to start understanding cross organisational learning is to use Huber's description of organisational learning in general as a framework for discussion. Huber lists 4 important contributing processes for organisations to learn [Huber 1991]:

1. Knowledge Acquisition
2. Information Distribution
3. Information Interpretation
4. Organisational Memory

We will review these processes in regard to the advisory service to better understand its potential and trade-offs.

Advisories and Knowledge Acquisition

In order to learn, new knowledge has to come from somewhere. An organisation can acquire knowledge by learning from processes inside the organisation, for example through the experience of colleagues, or by learning from experience of others in the organisation or from sources outside the organisation. For example, by helping a customer with an incident, the CSIRT staff will learn from the experience, and any new insights can then be shared among the team members.

New knowledge distributed in the advisory service is not acquired within the organisation, but rather comes from vendors that publish information about vulnerabilities and fixes or from other sources like CSIRTs and research groups. Such second-hand learning is referred to as vicarious learning [Huber 1991, p.96]. Hence, knowledge acquisition in the advisory service is dependent on acquiring information second hand. Many CSIRTs do not know exactly what kinds of systems are used by the constituency and for what purpose, and hence, the information gathered might not be needed or information that is indeed needed is not gathered. Even if the CSIRT did know the exact systems and requirements that are used in the constituency, they have often no way of knowing if they are in a hardened or vulnerable state. In addition most CSIRTs do not have the resources or the necessary information, such as source code, available to do their own vulnerability analysis.

The main weakness in the advisory service is therefore mainly related to the relevance and completeness of the gathered information.

Advisories and Information Distribution

Information distribution has two important effects. Firstly, the distribution leads the organisation to learn, and secondly, it adds to the breadth of knowledge in the organisation [Huber 1991, p.100]. Information distributed through the advisory service is traditionally based on a mailing list. Individuals in the member organisations sign up to a mailing list to receive the information in the first place, and in some cases, the intention is that these individuals will forward the information further into their own organisations to distribute the information to the appropriate recipients. In some cases, the recipient might not have access or authority to all systems within the organisation he or she belongs to. Consequently, the information is not acted upon.

The main weaknesses of the advisory service in regard to information distribution, is that there is no way of assuring whether the information is indeed reaching out to all relevant recipients in the constituency or if the information reaches them in time to still allow mitigation measures to be started ahead of any exploitation. It is also unknown whether when receiving the information the recipient is competent and capable enough to understand the relevance and to implement repairs

that reduce or remove the vulnerability on his own or whether it will depend on other parties. If other parties need to be involved, another loss of information might occur in the communication.

Advisories and Information Interpretation

Interpretation of information is "the process by which information is given meaning" [Daft, Weick 1984, p.294]. There are several aspects of this learning sub process we can highlight relative to the advisory service. Information is interpreted relative to existing cognitive maps [Huber 1991, p.102]. To assure the best possible interpretation, the CSIRT might translate advisories from English into the language used by its constituency, for example Korean or German. Nevertheless, an organisation that receives an advisory might consider the information irrelevant because it concerns a product they are not using in their networks, say a server using Linux Red Hat while they are relying on Windows 2003 Server.

Another aspect that limits the information interpretation is information overload. According to Huber [1991 p.104], "overload detracts from effective interpretation". In such cases, the information is more likely to be disregarded and instead, the recipient will rely on the existing knowledge, for example that the system is indeed secure.

But even if the receiver of the information does use the software the advisory is targeting, we cannot be sure whether the information is acted upon. Firstly, the system administrator might not consider the need to update her or his machines to be critical, and she or he might worry about any side effects a patch might cause. Secondly, she or he might already have fixed the problem prior to receiving the advisory. However, in the latter case, it is still an open question whether in the mean time any of the systems have been reconfigured or reinstalled without the patch. Thus, within the network a system can still be vulnerable, but the perception is that it is not.

From this discussion we can identify two additional key weaknesses with the advisory service with respect to information interpretation. Firstly, an advisory is not necessarily relevant either because it is not applicable, or because the organisation does not identify the information as useful (even if it is). Secondly, if it is not interpreted as very useful in general and the advisories that are indeed applicable might not be given the same weight as the existing knowledge base of the receiving unit that assumes their network is secure. This is because the information is not rich or clear enough to be given meaning [Huber 1991, p.103]. I.e. the recipient is not able to make a connection between the solution and the need for a solution.

In general not all CSIRT have a way of knowing which systems are used by its various constituents, and hence, targeting information is difficult in such cases. Similarly the security posture in general is often not known to the CSIRT either, making it very difficult to prove any concrete need to apply a particular advisory in most instances. Depending on the type of the CSIRT – coordinating vs. internal – the level of information available is varying, therefore these assessments might not apply to all CSIRTs in the same way.

Advisories and Organisational Memory

Organisational memory is the ability to store information and later to recall this knowledge accurately when appropriate [Huber 1991, p.105]. Current methods for storing and disseminating advisory information, provide very weak organisational memory for advisory services at best. The information may be stored on a public web page as well as in several e-mail accounts, but it is not very likely that the information will be recalled if needed, as many information owners will not know whether the systems have been changed and if the advisory might be useful in the future. The advisories are only sent again if there is a growing exploitation rate of the vulnerability it addresses

or more information becomes available, making it necessary to update the advisory. In that case it is usually sent again to the same recipients with an extra notification that it is critical due to a higher probability of exploitation or a reference to the updated section. The time between the first and the second time the same advisory is sent out, is usually short, as indicated by the analysis of the DFN-CERT advisories.

Because there is very little retrieval of the information, there is practically no organisational memory in the advisory service even though the information is stored and available. In particular, decisions to be made by the receivers need to be repeated and information re-assessed, each time the advisory information is re-sent. Without organizational memory this will take as much time and resources as the first assessment.

Summary of the advisory service as an cross-organisational learning process

We see that on all four learning sub processes (acquisition, distribution, interpretation and memory), the advisory service in a CSIRT has several weaknesses. From the description above we can conclude that the learning processes needed to make a CSIRT deliver an effective proactive service are indeed complex. Problems include delays for distributing information across organisational boundaries, the need for accumulation of information as memory, the fact that several feedback processes go beyond what the CSIRT can currently control, and that some learning feedbacks are simply missing.

The System Dynamics method was designed specifically to address issues with such attributes from a holistic perspective. It is therefore a good candidate approach for analysing such problems. In this paper we have only used conceptual modelling, but the future plan is to develop a running simulation model to give a more profound analysis of NBHW and the advisory service.

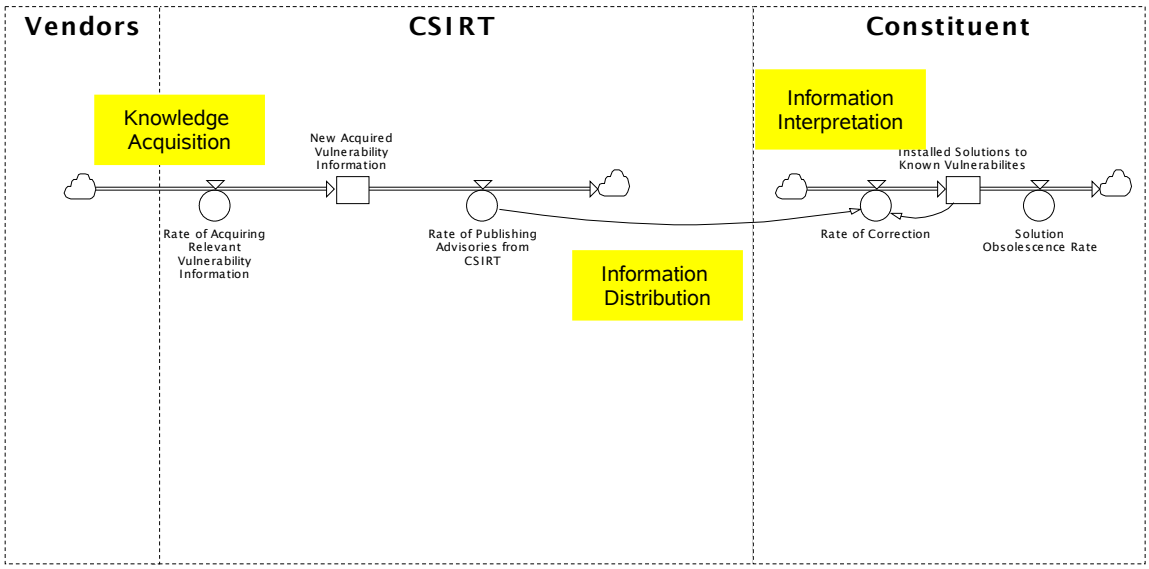

Figure 2: System Dynamic Model for the Advisory Service

The above graphic visualises the areas which can be attributed to the processes of organisational learning represented in the advisory service. In the model, we assume that the CSIRT will acquire relevant advisory information from vendors or others at a certain rate represented by a flow variable (*Rate of Acquiring Relevant Vulnerability Information*). This information flows into the CSIRT and

accumulates in a stock variable labelled *New Acquired Vulnerability Information*. This process represents the knowledge acquisition process, as highlighted in the diagram. The information acquired is information in process of being translated into the right format for the constituency and quality assured before it is sent out. The *Rate of Publishing Advisories from the CSIRT* is therefore the outflow from the stock of information in the process representing the information distribution process. The same rate is influencing the *Rate of Correction* for each constituent. However, we assume that there are significant losses of information in the transition from the information sent out to the information used to make a correction, owing to reasons discussed previously. Hence, this part of the model represents the information interpretation process. If the advisory is acted upon, it adds to the stock of *Installed Solutions to Known Vulnerabilities*. Gradually some of these solutions might be lost, as software can be reinstalled without the appropriate patches or configurations, for example.

The goal of the CSIRT is of course to keep the level of installed solutions at the highest possible level. However, two very important weaknesses can be highlighted in this diagram. Firstly, the loss of information through the information interpretation process is assumed to be a significant problem, indicating that the information interpretation, in particular, is very weak. Secondly, if an advisory is not acted upon, or if the constituents system for some reason removes a solution, there is no way the advisory service in its current form will enable the detection of the problem. The reason can be found in the in fourth learning process – organisational memory. This learning process is practically missing in the traditional advisory service. Furthermore, to enable such a process, additional learning feedback from the constituency is required. The CSIRT needs to know the actual state of the constituents' networks in order to recall the appropriate information for them, distribute the information again and make sure it is interpreted correctly in order for action to be taken to bring the actual (vulnerable) state of the networks into the desired (hardened) state.[2]

Taking into consideration what we have identified so far, there are certainly strategies to improve the advisory service. For a start the integration of an organizational memory as well as institutionalizing feedback loops to gain insights from the constituency would be valuable approaches. Therefore we will look at another proactive service to show a much more effective approach to hardening systems.

Organizational Learning and the Neighbourhood Watch Service

DFN-CERT started in 2005 to develop a new service called Neighbourhood Watch [Grabarske 2005]. Similar services are known to be established within some organisations, utilizing similar technologies but other organisational rules than those applicable for coordinating CSIRTs. The Neighbourhood Watch (NBHW) service has been developed based on four core components:

1. A vulnerability scanner that identifies existing vulnerabilities in constituents systems that can be reached over the network
2. A database of collected data consisting of historic as well as current information about the security posture of the constituent's systems
3. An assessment engine consolidating and evaluating the criticality of existing vulnerabilities and trends in perspective to historic data

2 We recognize that depending on the scope of the CSIRT the level of information about constituent systems might vary. In general for coordinating CSIRTs, especially for external CSIRTs like in national research networks, the level of available information is low. If the CSIRT is internal usually a higher level information can be assumed. Still, there is doubt that enough information is available if you are inside an organization if you have not prepared for making the information available and maintain it.

4. Concise reports that outline all vulnerabilities, put them into some priority based on their criticality and adds references to available advisories that explain these vulnerabilities and how to fix them.

In general any vulnerability scanner can be useful for identifying vulnerabilities [Schneier 2000, p.198-200] and they are an important part of the information security management process today [Egan, Mather 2005]. Many organizations use penetration tests to thoroughly analyze networks and / or hosts, depending on the negotiated scope for such tests.

To avoid constituent concerns about possible denial-of-service effects, NBHW is restricted to carry out only non-intrusive scans and probes. NBHW takes the viewpoint of any arbitrary attacker on the Internet, taking a cautionary look at hosts reachable over the network. The benefit of such tests is relatively easy to set up and to maintain, and it will in fact detect all information visible – and therefore available – from the outside.

The concept of NBHW was not to develop just another service, but to integrate it with existing services, therefore the reports also include information from the advisory service. By doing this in essence, NBHW supports a cross-organisational learning process that identifies known vulnerabilities in the constituency systems, points responsible administrators towards these vulnerabilities, and links this information to advisories describing available mitigation strategies, for example to apply a patch developed by a vendor.

By evaluating NBHW as an organisational learning process according to Huber's description, we can identify some key differences compared to the advisory service as a stand alone process [Huber 1991]. Remember that NBHW is partially based on the advisory service, and hence, some new learning feedbacks are created immediately that influence all of the four main sub-processes that were already introduced.

Neighbourhood watch and knowledge acquisition

The information about what vulnerabilities to scan for as well as available solutions are all obtained from vendors, and this results in the vicarious learning for the CSIRT. However, the scanning component of NBHW generates interesting information feedback to the CSIRT, as it will provide the CSIRT with information about the software used by the customers in the constituency. Hence, the CSIRT can allocate its resources more efficiently by acquiring more relevant information as well as spending less time on irrelevant information.

A core aspect of NBHW is obviously that it identifies vulnerabilities in constituent networks and allows a connection to be made with the constituents that can be used to inform them about relevant solutions. The CSIRT will therefore acquire information from the constituents as well, making the customers networks much more tangible both for the CSIRT and the constituents themselves. Thus, the perceived state can be assessed much more realistically by comparing it to the de-facto state of the networks. This type of learning is what Huber refers to as performance monitoring [Huber 1991, p.97].

In addition to routinely scanning organisations that signed up for the service, NBHW provides the potential to scan the same constituents in an ad-hoc fashion, i.e. in addition to the ordinary schedule, if this is considered necessary. Such needs might arise, if an early warning system shows a new worm outbreak which is already under way and exploiting particular vulnerabilities. An ad-hoc scan concentrating only on these vulnerabilities will promptly provide a list of systems exposed to the worm – and which might in fact be already compromised.

If we compare NBHW to the pure advisory service, the most valuable part of NBHW is not just the new information that is acquired, but rather that this information is synthesised by mapping the vendor information and solution about a vulnerability to an actual vulnerability identified in a customer network. Thus, the synthesised information leads to new insights for both the customers and the CSIRT. The relevance of the information is significantly increased as no irrelevant information is provided. In addition, the system will create some learning feedback to the CSIRT about any new constituent software, thereby increasing the relevance even more Thus, NBHW significantly improves the weaknesses of the advisory service as long as the vulnerabilities are visible over the network.

In addition, as the CSIRT has the same information as its customers, they can also follow up if they do not see any action taken on the received information over some period of time. Hence, it is easy to identify and prove a point for the need of new customer routines to take action on the information generated by NBHW. Again, we see how NBHW potentially can facilitate, enhance and help to create even more learning loops in the system.

Neighbourhood watch and information distribution

While the advisory service distributes information through a mailing list, NBHW is providing a web interface containing identified vulnerabilities and corresponding solutions, as well as highlighting changes (new systems, new ports, etc.) since the last routine scan. Obviously, as the information is sensitive (in particular the identified vulnerabilities), the access to the system has to be protected by using a PKI[3] based authentication scheme, transport encryption and access controls.

Neighbourhood watch and information interpretation

In the advisory service, the understanding of vulnerability information might differ significantly between the CSIRT as the sender of an advisory and the receiver of this information (the constituent). NBHW might reduce this gap significantly for both sides. However, due to synthesised information in NBHW it will be easier to interpret its relevance, and the risk of overload is significantly reduced as only applicable information is presented.

The rapidity of feedback in a system enhances learning [Huber 1991; Sterman 2004]. Dependent on the frequency of scanning, NBHW can provide very rapid feedback to both the CSIRT and the constituent, something that can significantly enhance the interpretation. The perceived state about the constituent networks is brought much closer to the actual state as the delay in the feedback is significantly reduced by the scanning frequency.

NBHW can also contribute to changing the mental model of system administrators and the way they perceive the state of their networks. As constituents immediately realise that they **are** vulnerable, their willingness to take correction measures might change significantly. Research shows that a significant gap between perceived low risk and actual high risk in a system can emerge if people do not experience any problems [Sawicka, Gonzalez 2003]. Such an "out of sight out of mind" mentality can therefore reduce people's willingness to take action before it is actually too late.

However, it is generally very difficult for people to change their mental models [Sterman 2000]. Even if NBHW did succeed to change system administrator behaviour with respect to institutionalising more proactive measures, it will most likely happen only with long time delays; even when compelling evidence is available. A lot of "unlearning" has to take place. That is, people

3 PKI is an abbreviation for "Public Key Infrastructure". PKI is used for persevering information integrity, confidentiality and availability. DFN-CERT is also providing a PKI service to its customers.

have to first disregard what they considered to be the "truth". For example that they are invulnerable because they have not experienced any significant incidents, before they can make progress in this area.

Neighbourhood watch and organisational memory

Organisational memory has two main components [Huber 1991, p.105]: Information storing and Information recall. In general the human capacity is limited to support these functions, as we argued in the discussion of the advisory service. Organisations typically try to use operating procedures, routines and scripts to support both processes to compensate for human weaknesses. Huber suggests that computer-based organisational memory has considerable potential, for example by diagnosing quality problems and by being able to locate information to remedy any problems identified. In a CSIRT context, we might even consider it a prerequisite for organisational memory.

NBHW can serve as an important organisational memory for the constituency it serves. First, it can store information about vulnerabilities and corrective measures. As NBHW utilizes CSIRT standards (EISPP for the advisory itself and CMSI to reference systems and software [Grobauer 2005]) existing information like the collection of advisories from DFN-CERT since 2003 are readily available for use. This type of example shows that much needed information has already been accumulated.

Through scanning constituent systems, the CSIRT identifies vulnerabilities and maps them to corrective information. NBHW stores the history of these scans and can thereby highlight changes since last scan.

Summary of the NBHW service as an cross-organisational learning process

Compared to the advisory service we see that all four learning sub processes (acquisition, distribution, interpretation and memory) are present. The NBHW has several advantages as an addition to advisory service. Still there are delays to be expected, but the advantages are considerable, such as providing much better means to raise the security by hardening more systems much quicker than before.

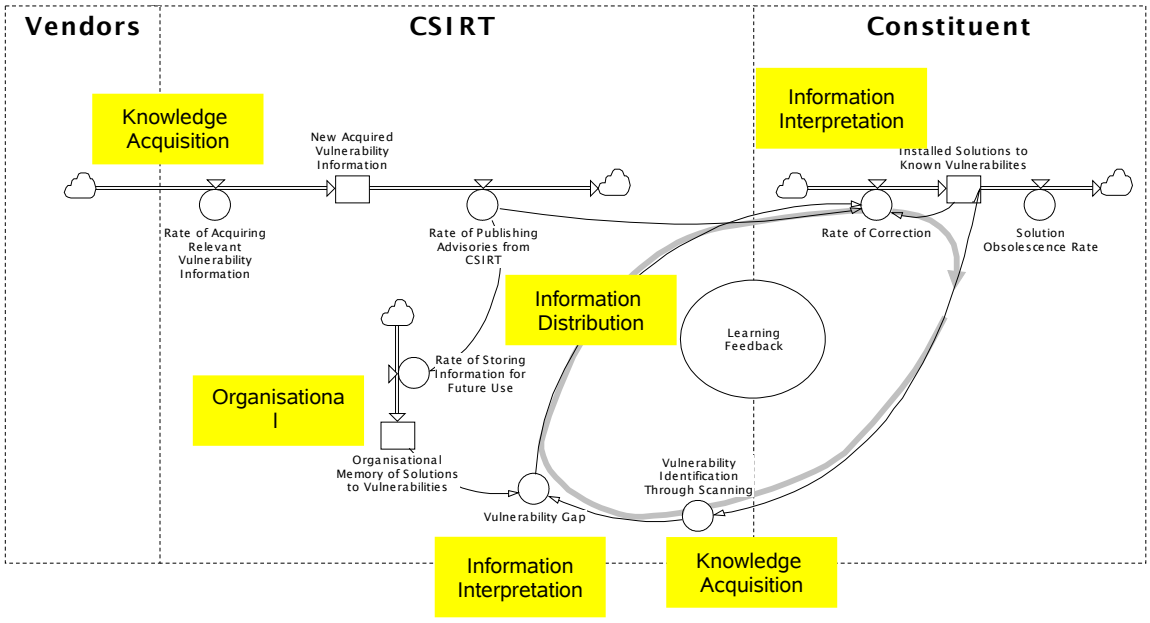

Figure 3: System Dynamic Model for the Combination of Advisory Service and Neighbourhood Watch Service

An additional stock of *Organisational Memory* has been added to this figure. The inflow is identical to the publication rate of advisories. Hence, the stock represents the accumulated number of past advisories that can be used again and again if needed. Through scanning, the CSIRT can now acquire additional knowledge about actual vulnerabilities in constituent networks. Thereby a vulnerability gap between the actual (vulnerable state of constituents networks) and the desired (hardened state if all advisories in the organisational memory have been followed), can be identified for both newly discovered and old vulnerabilities. Identifying the specific vulnerability gap is actually a matter of synthesising information into new knowledge. The advisory information will thereby most likely be interpreted in the new way for both the constituency and also for the CSIRT. In other words, the CSIRT knows about specific problems in the constituency and will act accordingly. In NBHW the information will be distributed through a web interface where the new synthesised information is provided. Hence, the probability that action will be taken to correct the problem by constituents is much higher. However, if this is not happening for whatever reason, the CSIRT can through further scanning identify that no action is taken and thereby manually follow up with a specific constituent to find out why in order to close the vulnerability gap. This closes a goal seeking feedback loop where learning continuously takes place. The goal will continuously adjust towards a moving goal, which is the stock of organisational memory of solutions to vulnerabilities (i.e. mostly past advisories). As an addition to the advisory service, NBHW will thereby significantly improve the main areas of weakness in the traditional stand alone advisory service: Information interpretation and organisational memory across organisational boundaries.

Conclusions

While the advisory service works fairly well with respect to acquisition, and distribution, it is rather weak in helping constituents to interpret the information as relevant or not, and most importantly, there is no organisational memory provided to or within the organisations in the constituency. Historically this has not posed any problem if the constituency was adept enough to benefit from the advisories as they were. Only with the introduction of advisory services for non-technical users have some of these problems became obvious, limiting the usefulness and the adoption of this service outside the technical community.

Potentially, the NBHW service will help to significantly reduce the weaknesses of the advisory service in that it provides the necessary organisational memory for how to stay protected, but it also helps interpret which advisories are relevant by identifying vulnerabilities in the outer perimeter of the constituents' networks on a regular basis. In addition, it automatically feeds back information about the needs in the constituency to the CSIRT which can then, in turn identify and distribute even more targeted and relevant information.

Therefore our recommendation to all CSIRTs is to review their proactive services carefully and assess, if they are useful – or if they need to be re-engineered based upon the concepts we have introduced above. The advisory service will be easily improved by taking our analysis into consideration.

As an additional recommendation for all CSIRTs it can be suggested to take-up other proactive services, like the NBHW for one example, which provides more robust feedback between all parties concerned and therefore possess a huge potential for delivering up-to-the-point information in a way that is more readily consumed and appreciated by the receivers.

However, as a cautionary note, different service models need to be considered. And while the potential might be huge, the real benefit is often determined by other factors. In relation to the NBHW for example, as a service that requires constituents to sign-up for the service, its overall effect on the constituency is very much dependent on the customer take up rate.

Just as NBHW and the advisory service interact, we expect that the relationships of these and other services provided by a CSIRT are worth exploring to identify strategies to improve them or to create value added not achievable before.

Acknowledgement

As always were are thankful for the ongoing support of the IRT team (Andreas Bunten, Jan Kohlrausch and Klaus Möller) within the DFN-CERT in regard to our research topic in general, as well as for the support of an old DFN-CERT Fellow, Wolfgang Ley, now with SUN.

We thank for the intense reviews by Robin Ruefle and Georgia T. Killcrece, both with the CSIRT Development Team at the SEI.

And we would also like to thank Jens Grabarske, DFN-CERT, and Till Dörges, PRESECURE, as the people that brought the NBHW concept to life.

References

Abdel-Hamid, T. a. and S. E. Madnick (1991). Software Project Dynamics - An Integrated Approach. New Jersey, USA, Prentice Hall Software Series.

Arbaugh, W. A., W. L. a. Fithen, et al. (2000). "Windows of Vulnerability: A Case Study Analysis." Computer **33**(12): 52-59.

Daft, R. L. and K. E. Weick (1984). "Toward a Model of Organizations as Interpretation Systems." Academy Management Review **9**: 284-295.

Egan, M. a. and T. Mather (2005). The Executive Guide to Information Security - Threats Challenges, and Solutions. Indianapolis, Addison-Wesley.

Grabarske, J. (2005). Neighbourhood Watch. 12. DFN-CERT Workshop 2005. Hamburg, Germany.

Grobauer, B (2005) CVE, CME, ... CMSI? Standardizing System Information. 2005 Annual FIRST Conference. Singapore.

Huber, G. P. (1991). "Organizational Learning: Contributing Processes and the Literatures." Organizational Science **2**(1): 88-115.

Killcrece, G., K.-P. Kossakowski, et al. (2003a). Organizational Model for Computer Security Incident Response Teams. Pittsburgh, PA, USA.

Killcrece, G., K.-P. Kossakowski, et al. (2003b). State of the Practice of Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA, USA, CMU/SEI.

Lipson, H. (2002). Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. SPECIAL REPORT CMU/SEI-2002-SR-009. Pittsburgh, PA, USA.

Sagan, S. D. (2004). "Learning From Normal Accidents." Organization and Enrivonment **17**(1): 15-19.

Sawicka, A. a. and J. J. Gonzalez (2003). Choice under risk in IT-environments according to cumulative prospect theory. Twenty-first International Conference of the System Dyamics Society. New York, System Dynamics Society.

Schneier, B. (2000). Secrets and Lies - Digital Security in a Networked World. New York, Wiley Computer Publishing, Johan Wiley & Sons, Inc.

Sterman, J. D. (2004). Business Dynamics - Systems Thinking and Modeling for a Complex World. Boston, Irwin McGraw-Hill.

van Wyk, K. R. a. and R. Forno (2001). Incident Response. Sebastopol, CA, USA, O'Reilly and Associates Inc.

West-Brown, M. J., D. Stikvoort, et al. (2003). Handbook of Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA, USA, CMU/SEI.

Wiik, J., J. J. Gonzalez, et al. (2004). Dynamics of Vulnerability. Twenty-second International Conference of the System Dynamics Society. Oxford, UK, The System Dynamics Society.

Wiik, J., Kl.-P. Kossakowski (2005a) Dynamics of Incident Response. 2005 Annual FIRST Conference. Singapore.

Wiik, J., J. J. Gonzalez, Kl.-P. Kossakowski (2005b) Limits to Effectiveness in CSIRTs. Twenty-third International Conference of the System Dynamics Society. Boston, The System Dynamics Society.