CyTRAP Labs

Building an Early Warning System (EWS) that works or how to skip the ropes[1] [2]

Keywords: awareness, benchmarks, culture of security, early warning system, EWS, incident response, information assurance, Key Performance Indicator, KPI, malware, prevention, public policy, risk, risk management, security assurance, security metrics, threats.

Research suggests that our level of preparedness to recover the internet following a catastrophic cyber disruption is inadequate. In particular, some countries are not sufficiently prepared for a major attack, software incident or natural disaster that would lead to disruption of large parts of the Internet (see also: are we prepared against an internet attack of disastrous proportions? – http://www.casescontact.org/euist_view.php?newsID=4030)

The myth would have you believe that an early warning system (EWS) will make a difference regarding security posture and better protection of information assets by citizens and SMEs. Moreover, some governments would feel that such efforts address the security challenges for "A single European Information Space" adequately (the seven myths about Early Warning Systems see http://cytrap.eu/blog/?p=64).

But even if falling in the trap regarding the myths as outlined above, a successful EWS that succeeds in leveraging its resource advantages takes planning, careful implementation of the former and, as importantly, regular performance assessment. Below we will offer some ways on how an EWS can be set up and operate while helping in raising awareness and providing the tools that support users to better protect their information assets. This paper is one small step on the long journey for a higher level of awareness regarding security by users and, most importantly, leading to improved prevention.

Who is our Target Group

Before launching an Early Warning System (EWS) one must define the objectives for such a venture in order to be able to assess if it was a success thereafter (see here: Continuous improvement of an EWS - the key to success - http://cytrap.eu/blog/?p=34). In fact, it is important to begin addressing

[1] The author would like to thank Francois Thill (http://www.cases.public.lu) for his insightful comments made on an earlier draft of this paper. Omissions or misunderstandings are, of course, the author's sole responsibility.

[2] A shortened version of this paper was published as Gattiker, U. E. (Jan-Mar 2007) Building an effective early warning system. **ENISA Quarterly Vol.** 3, No. 1, 6-8

CyTRAP Labs

these issues better now than later[3]. Only such an approach will help in better preparing users for the next next malware pandemic that will surely happen in the not so distant future.[4] In most countries governments have taken the stand that providing information security warnings and other help to citizens is similar to a nation's public health efforts. Hence, such information and services must be provided in some form or another to help reduce the risk for pandemics. Nonetheless, every EWS must harness its limited resources effectively to create major advantages and, in turn, show superior performance.

Also, providing information that helps improve preventive skills of a Small and Medium-Sized Enterprise (SME) or a self-employed person is somewhat different, than what is needed to improve security for a family's PC. But even within a family, the most effective approach differs according to what member of the family one chooses to communicate with. For instance, teenagers tend to prefer Instant Messaging for communicating, while silver surfers[5] use e-mail for the most part. Such differences do, of course, have major implications regarding awareness raising and prevention.

The Checklist presented below addresses these issues in some more detail by focusing on eight critical areas (1-8) that must be addressed in order maximize added value of an EWS.

Awareness Raising will Help But….

From economics and marketing we know that diffusion of a technology (i.e. how many of one's friends use it already) does influence the likelihood of non-users taking up the use of a new gadget or gizmo. As such, every teenager has a mobile phone and friends can and are contacted using SMS or voice. Hence, awareness raising and prevention for this group of users regarding security of information with mobile phones is most certainly a good first step.

Similar to mobile phone technology, people will take advantage of e-government or online banking services, if they can see a benefit to themselves. An example might be that the use of e-banking helps save time and/or reduces service charges levied by the bank[6].

---

[3] Unless the target population for an EWS is clearly defined, subsequent performance levels may be erratic from a particular stakeholder group's perspective (e.g., is this alert helpful to home users or Small and Medium-Sized Business Enterprises (SMEs). We have discussed this here: Debunking mania - early warning systems and better security (http://cytrap.eu/blog/?p=29).

[4] Organizations that already help us reach this goal are such as, CSIRTs, CERTs, WARPs and others as we have discussed here: Do CERTS differ from WARPS or should we create something different (http://cytrap.eu/blog/?p=50)?

[5] This term is difficult to define (e.g., at what age does one become a silver surfer?). Age may be an important moderating or mediating variable for assessing internet and technology use. However, at a later stage in life, being either part of the workforce or having retired may be a factor that is far more important for determining awareness and information security needs and demands than age. Hence, one might control for the effect of age upon security preventing but work stats (working full-time vs. not) could be the decisive moderating variable.

CyTRAP Labs

A similar line of reasoning can be used for an EWS, whereby the latter must:

1) focus on services that satisfy its target group (s) (e.g., teenagers versus silver surfers or SMEs versus large organizations)

2) provide services that help users to better manage risks and improve information security, while keeping a user-friendly approach in mind

By following the above criteria, an EWS should help users getting the information they need in order to reduce, for instance, the risk of becoming a victim of a phishing attack or identity theft[7]. However, it is still questionable if these educative and informative efforts will also immediately increase the uptake ratio of a particular service like e-government or e-health services. But using a longer time horizon, better know-how about the risks and better prevention efforts will, most certainly, help alleviate citizens' possible fears and mistrust that may today prevent them from using these services.

Awareness raising must always be targeting a clearly defined user group that, based on its behaviour, is vulnerable to a specific threat (see Checklist below). To illustrate, youngsters being unaware that their Bluetooth connection on their mobile phone is turned on makes them vulnerable to specific attacks. Accordingly, in order to reduce this vulnerability, users should first be aware that this vulnerability exists and, second, change their behavior by switching their phone's Bluetooth off when not needing it.

The above illustrates that if awareness raising efforts are fructuous, they will result in behavioural change. Consequently, being aware of a threat one might be exposed to is an important first step towards security. Nonetheless, changing one's behaviour is the key on the road to better security because only that will reduce one's risk exposure towards becoming a victim of an attack.

Insert Checklist about here

The above checklist indicates that eight criteria must be addressed to minimize the risk for failure. The latter would occur if awareness raising efforts regarding users' security posture would not result in the behavioural changes required to achieve the objectives as specified at the beginning of the project including the security metrics and key performance indicators (KPIs) that will be used to determined the success of the project.

---

[6] The primary reason for banks to offer automated teller machines (ATMs) in the early 1980s was to make banking more attractive for younger clients that wanted to have access to these services even after office hours. Those clients are also the ones who will generate the revenues banks need by requiring mortgages and other types of financing.

[7] Hence, it is not wise to make one of the EWS' targets the raising of awareness about how to do safer online banking for people who are not currently using it. This task should be left to financial service providers who have a vested interested in not only protecting their customers' information but, as importantly, improve the services the provide in a competitive market.

CyTRAP Labs

Safer Surfing Requires Behavioral Change –Good Key Performance Indicators (KPIs) can Help

Focusing the EWS services to the target group one wants to reach is critical. It is also obvious that the information provided (see point 2 in the checklist above) should be specially customised in a form and format to the targeted community. Making users change their online behaviour to reduce their risk for becoming a victim of attacks must be a key issue (see point 4 in our checklist). Hence, awareness efforts should focus on how much awareness raising has and continues in helping people use more secure behaviours to reduce their online risks. Knowing about privacy and security is great but handling those issues following best practice is better. In turn, KPIs cannot stop by measuring how successful awareness raising campaigns are but, instead, must also address and measure how much behavioural change can be related to these efforts. An example could be to assess if the awareness campaign reduced the reported cases of identity theft or the number and sizes of botnets that were discovered.

It is difficult to come up with a framework that is most appropriate across situations and scenarios because local circumstances may influence local needs strongly (e.g., regulatory, cultural, educational differences as well as experience and prevalence of certain types of threats in a region). Nonetheless, we do know from marketing and sales that a dedicated team is critical to success. In fact some would suggest that discontentment about information security levels tends to drive the staff in wanting to do something about it. Accordingly, there is no point in finding a new vision that can be implemented with the help of an EWS if you are not angry enough to want it to happen. Moreover, different settings and services provided require different types of skills from staff. To illustrate, the technical level that must go into an advisory for home users is surely different than what is required for a system administrator in an SME [this is addressed in some detail here - 4 Tips for building an effective Early Warning System - organizational and human resource issues (http://cytrap.eu/blog/?p=63)].

Following the above reasoning it appears obvious that in order to give an EWS the chance for serving citizens and SMEs, a dedicated staff is needed. These individuals must not only be familiar with the equipment their clientele uses but also understand the context and environment (e.g., SME or home office) in which these information assets must be protected.

Why Benchmarks Could Fail Our Efforts

As one might conclude from the above, the identification and developing of key performance indicators (KPIs) is a challenge to say the least. KPIs and benchmarks applied regarding awareness raising and behavioural changes must help assess how effective these efforts were in helping reduce risk and mitigate threats for target groups (e.g., citizens and SMEs) regarding cybercrime, malware and hacking attacks. Moreover, what is required to accomplish greater security and trust is different across user groups and settings (e.g., SME versus home PC). Therefore, the KPIs or security metrics used to assess the effectiveness of such efforts must differ across settings. Key Performance Indicator(s) cannot be solely based on number of people receiving a security tip, guide, alert or having been

CyTRAP Labs

informed via the media. A more practical KPI is one that focuses on measuring the outcome (e.g., behavioural changes by users due to awareness raising interventions) based on certain activities[8].

Because of this, security metrics are types of key indicators that are becoming increasingly important in the IT security and risk management field. Such metrics help in assessing the effectiveness of awareness campaigns and the implementation of security policy in organizational settings. For instance, large corporations tend to use such security metrics as[9]:

- viruses detected in user files	92.3%
- viruses detected in e-mail messages	92.3%
- invalid logins (failed password)	84.6%

While these numbers are definitely important, their usefulness from a strategic and policy level are limited. For instance, while virus files may be detected, having an updated anti-virus program mitigates this risk considerably. Not clicking on the virus-infected attachment further reduces this risk. As importantly, not having administrative rights on one's user account does not give one permission to run a so-called .exe type of file that might be attached to the e-mail. Hence, if done right children are given a user account on the family's PC that enables them doing instant messaging or surfing the internet but, most importantly, it does not grant them permission to install or remove programs. This again reduces the risk of having a virus raise havoc on a home PC. Unfortunately, none of the three examples of metrics listed above give us the information we need to evaluate our efforts properly. In turn, they do not provide us the insights required for fine-tuning future awareness raising efforts initiated by an EWS or another agency.

The above illustrates that unless the security metrics developed and applied during assessment provide information about users' permission levels, their value for security policy could be limited. Similarly, surveying users and asking them about if they have experienced a virus problem in the last few months is interesting. But it does not indicate if their multi-layered security efforts prevented the infection from causing any damage. A cross-European study reported such findings and demonstrated, in turn, the limited value of such information for policy-makers[10]

As well, regardless if the KPIs used are called benchmarks, security metrics or something else, they must be linked to the efforts undertaken by, or performance targets given to, an EWS. To illustrate, if

[8] To illustrate, a practical KPI is one that assesses the number of botnets in a country using home PCs for criminal activities as well as the average number of PCs that are part of such botnets before and also after an awareness raising campaign. Similar measures refined according to need can be used to assess awareness campaigns against identity theft, phishing attacks, safer surfing, more secure online banking and so on (see also CyTRAP Labs KPI set of benchmarks for awareness raising, http://CyTRAP.eu/blog).

[9] Gattiker, U. E. (October 17, 2006). CyTRAP Labs - guide - developing IT security metrics that work for you (http://cytrap.eu/blog/?p=61). **Information Security this Week**, Vol **7**, Nr. 40.

[10]The study is described here: Info Security - Confidence and Trust - A Cross-Sectional Study – Europe June 2005 - including the free report for download (http://casescontact.org/euist_view.php?newsID=3712)

CyTRAP Labs

an awareness campaign is being prepared, how will its success be measured? What will decide if the campaign was a success or not. Discussions about these issues must culminate in a precise, succinct and short description outlining what indicates success versus failure. For instance, one has to agree if a security metric trying to assess the reduction in the number of botnets out there is a useful benchmark. And even if it is, by what percentage must this number be reduced, within what time frame, in order to claim success for the awareness campaign? As points 7 and 8 in the checklist already suggest, a highly standardized cross-national approach is difficult to pursue. For instance, one country for good reasons might be concerned about botnets. Another might be worried about patching because a vast majority of user's run Windows 98 for which Microsoft no longer issues security patches. In another region, patch latency might be so big because a large percentage of home users uses dial-up connections to go on the internet. In turn, using the same measuring stick makes little sense if different contexts result in different threats that must be addressed in two regions.

Security experts and risk managers sometimes forget that difficult and complex issues must be resolved before agreeing on a set of security metrics. Otherwise their usefulness could be questioned once the information has been collected. Worst could be that the figures obtained indicate that the informational value of the security metrics used for policy- and decision-makers is limited.[11]

Conclusion and the Future of Early Warning Systems

Unfortunately, most public EWS services, regardless of the target group they try to reach, provide the same fare regarding awareness raising and prevention services. Surely, SMEs have different needs than government departments. As well, home users are not a homogenous group (e.g., silver surfers use different applications than the family's teenagers). Hence, to gain a resource-advantage the target market(s) must be identified carefully, in order to provide relevant information that is seen as providing added value. Moreover, to make available a product or service that will remain in high demand, continuous, incremental innovations and service improvements are required. In turn, these can cumulatively have a major impact on the performance of an EWS over 12 to 18 months.

As our checklist points out (especially points 7 & 8), Gmail, CyWorld, Myspace, Skype, and other Web 2.0 developments are new services that are starting to become the next disruptive technology for CIOs (Chief Information Officers) and policy makers. Young employees were the first that began using these services from home and whilst still being students. They are now bringing these tools and methods with them into the workplace. Instant messaging is one example, where the ever greater use by teenagers and students has eventually brought this technology into the workplace. Moreover, its use is becoming ever more prevalent. Naturally, the threats coming with this technology must be addressed as well.

For an EWS the challenge will be to provide support and intervention that helps companies to adopt new communication technologies, while managing risks and threats effectively. Nonetheless, better security and privacy protection for citizens, employees as well as their firm's customers is needed to

[11] Gattiker, U. E. (December 6, 2006). CyTRAP Labs – guide - the seven deadly sins of security metrics (http://cytrap.eu/blog/?p=95). **Information Security this Week**, Vol **7** Nr. 50.

CyTRAP Labs

achieve not only legal compliance but as importantly, manage risks more effectively[12]. Unless we customize awareness raising and prevention efforts according to the various groups' needs, added value of these campaigns, publications and/or services will be limited. Besides, security metrics must be identified that can be linked to the strategic targets set. As well, metrics used must be based on objectives that can be quantified and defined beforehand. In turn, a clear link between awareness efforts and behavioural change as measured by agreed upon security metrics are a key ingredient on the long journey to success.

We may hope for using one approach to improve security posture across many settings (e.g., regions, countries or user groups). But depending upon applications (e.g., e-mail versus instant messaging), type of internet connections (e.g., broadband - cable vs DSL or dial-up phone) and user groups (e.g., silver surfers vs teenagers), the types of threats and risks against privacy and information security will surely differ. Moreover, identifying the critical threats of today does not mean being prepared for tomorrow. Threats change with new applications and technologies. Nevertheless, while things change much remains the same, namely the objective to help protect citizens' rights for privacy. In turn, we may be able to agree on a cross-national set of security objectives but we surely must be flexible enough to allow participants to use different ways to get there, otherwise our efforts are prone to fail.

Finally, unless indicators such as KPIs or security metrics are clearly tied to policy objectives, why collect such information? Put differently, being unable to interpret findings coherently because moderating variables, such as user's age or type of operating system (e.g., Windows 95 vs. Windows XP versus Linux) and software used (e.g., open source and Microsoft Office) have not been collected and can therefore not be controlled for, conclusions drawn from such findings may cause more questions if not outright confusions than clarifications. Here, some European countries' efforts to move away from Windows will surely result in the need for different strategies to be used for achieving better information security. To illustrate, France's push to use open source in public administration (see http://cytrap.eu/blog/?p=114) will result in different security risks and outcomes for home users, than in a country where government agencies continue to work with Microsoft products. Hence, neither awareness campaigns can be the same nor the benchmarks used. Once these issues are addressed, however, KPIs have an important part to play to assess awareness campaign efforts' effectiveness. As well, they help an EWS and public-policy makers to fine-tune efforts, in order to improve information security and safety for target populations.

Bio

Urs E. Gattiker, Ph.D. is the CTO of CyTRAP Labs, a provider of security services, and the author of the 'The Information Security Dictionary – Defining the Terms that D Security for E-Business, Internet, Information and Wireless Technology'. He is director of CASEScontact.org an EWS for citizens and SMEs. You can read more of his writings at www.blog.CyTRAP.eu

[12] See also CyTRAP Labs - 10 reasons for why information security makes economic sense http://cytrap.eu/blog/?p=47

CyTRAP Labs

CHECKLIST - Awareness raising and prevention – eight steps to success

Benchmarks and security metrics are needed for assessing performance and added value provided by an EWS. To address security metrics strategically, however, some critical issues must be discussed and defined succinctly beforehand. We outline these below.

1) **Define which target groups will be served**

Likely result if ignored: Lack of sensitivity to differences in users' needs, wants and preferences reduces the value they will give to content and output produced. What a silver surfer might need is not what a teenager could be interested in regarding IT security.

Possible solution: Target groups must be identified clearly (e.g., home users and SMEs), thereby enabling the EWS to provide content that is seen as being highly relevant and helpful by the group to be served.

2). **Provide content that is written in a language easily understood by the identified target group**

Likely result if ignored: What a technical person needs to know makes little sense to a non-technical user. In fact, the latter may just not read the advisory being provided if it is too technical. As well, if it is not technical enough, a system administrator may neither trust the source nor have confidence in its output.

Possible solution: Use the language of the target group and separate technical from non-technical information if the former is desirable for home users that want such information.

3) **Alerts and warnings are issued in a timely fashion**

Likely result if ignored: Users could have been informed by the local news cast before they receive the alert from the EWS. This does neither increase trust nor confidence in the services offered.

Possible solution: Either avoid distributing warnings or else make sure that high quality advisories can be issued timely (e.g., within 8 hours after experts know about threat) including during long public holiday weekends (e.g., Easter Holidays and Christmas / New Year).

4) **Services help improve one's security posture**

Likely result if ignored: Better protection is unlikely to occur if the user does not begin to change his or her risky behaviour regarding spam or phishing mails.

Possible solution: Focusing on providing information that can be immediately applied for improving prevention. An example would be issuing security guides that outlined to a user in easy to follow

CyTRAP Labs

instructions a workaround for mitigating a threat identified today, before the vendor releases the necessary patch in about 15 – 120 days or so.

5). **Refrain from duplicating existing services but strive for added value instead**

Likely result if ignored: Issuing virus alerts duplicates vendor services and, therefore, is unlikely to add much value. Also knowing about today's Trojan does not prepare the user for the next pandemic.

Possible solution: Identify and define a service or niche that will add value in the eyes of today's subscriber and tomorrow's reader. In turn, refraining from duplicating will increase the value for the recipient.

6) Identify performance targets including the security metrics that support reaching strategic objectives.

Likely result if ignored: Hoping for A while rewarding or putting resources and efforts into B lowers performance. An EWS may get funding for an awareness campaign, while the funding agency is hoping that home users become more cautious in protecting their information to cybercrime (e.g., password, username, national ID number and banking information).

Possible solution: A security metric must be developed that helps assess the awareness campaign's effectiveness in achieving a lower number of reported cases of identity theft in the target group. Hence, the strategic objective and how it will be operationalised for measuring performance (i.e. security metrics to be used) has to be identified before launching a campaign.

7) Security metrics or key performance indicators (KPIs) that fail to take mediating and moderating variables into consideration

Likely result if ignored: Data collected via a user survey in regions A, B and C may suggest that 80, 90, and 50 percent of respective respondents indicated that they had at least five or more serious virus incidents within the last year. But this finding in itself can be rather meaningless unless…

Possible solution: It might be advisable to check and control for the possible effect in cases where respondents' had their Internet Service Provider (ISP) scan their incoming and outgoing e-mail for malware infection(s). Other control variables might be age and gender. Once these factors have been controlled for it might be very interesting to find out what moderating or mediating effect an awareness campaign could have had regarding the dependent varfiable – malware infections during last year.

7) Identify performance targets that enable participants to use different approaches to reach them.

Likely result if ignored: Related to point 6 above, besides that one must control for the possible effect on malware incidents due to the scanning of e-mails regarding malware by the ISP, particular situations might require different approaches regarding awareness and prevention.

CyTRAP Labs

Possible solution: Similar performance targets across settings should be identified if appropriate but, most importantly, differences must be taken into careful consideration. To illustrate, if botnets are an issue in one region, an awareness raising campaign may indicate success by revealing a clear drop-off of the discovered botnets after the campaign was launched. In another region the prevalence of wireless networks used in private homes might, however, suggest an awareness campaign focusing more on this issue than on botnets. If 40% of users have PCs operating using Windows 2000, 98 or 95, issues could also differ compared to Windows Vista which must be taken into considering when launching activities and trying to measure performance thereafter.