MEETING THE GLOBAL CHALLENGES OF SECURITY INCIDENT RESPONSE

Vijay Masurkar,[1] Simone Fischer-Hübner,[2] and Morton Swimmer[3]

[1]*Sun Microsystems, Inc., Burlington, MA, USA;* [2]*Karlstad University, Karlstad, Sweden;*

[3]*IBM Research Laboratories, Zurich, Switzerland*

Abstract: Responding to computer security incidents has become a critical function within an information technology program of any enterprise. These incidents are threats not only to computing equipment but also to the stability of establishments, such as small to large governments or utilities serving large populations. New types of security-related incidents emerge frequently and massive activities take place across the globe to mitigate the violations of security policies or recommended security practices. In spite of the concerted efforts from many organizations, complete solutions are still lagging behind. Proactive or predictive research and planning activities are on the rise in many industrialized nations. However, they seem to fall short on coping up with an unexpected global incident before incurring a substantial damage. What can the global security-aware organizations and communities do? This paper is intended to help set the stage for a panel discussion to be chaired by the first author with the members of the IFIP WG9.6/11.7, "IT Misuse and the Law".

Keywords: Security, Incident, Attack, Response, Global, Risk, Vulnerabilities, Legislation

1 INTRODUCTION

Since the Internet Worm of 1988 (Spafford, 1988), the world has seen quite an acceleration of security attacks as the Internet proliferated globally. New types of security-related incidents emerge on a frequent basis and massive activities take place across the globe to mitigate the violations of security policies or recommended security practices. Most local and national

Y. Deswarte et al. (eds.), *Security and Protection in Information Processing Systems*

governments recognize the need to protect their infrastructures and citizens (West-Brown et al, 1999). In addition, many also are aware that it is not enough to address such incidents only at their local level. Besides technological challenges, the socioeconomic and legal challenges are crossing national boundaries. Let us take look at the current state of security incidents and response capabilities, and briefly review the factors that help prevent or mitigate risks arising from these incidents. This review is intended to highlight the points for starting the proposed panel discussion.

2 CURRENT STATE: SECURITY INCIDENT RESPONSE CAPABILITIES

There are many known security threats to computing or networked resources. Perhaps the most common are port scanning, denial-of-service (DoS), IP address spoofing and sniffing, and injection of viruses, trojan horses or worms. With readily available tools and information on the Internet, finding specific vulnerabilities for a system is not very hard. Publicly available vulnerability assessment tools such as Nessus (2004) can be used to quickly identify where these threats are likely to gain a foothold and cause problems. Hackers also use port scanning tools such as Nmap (2004) to search through various network devices looking for ports that are open or enabled. They can compare this information to known, published vulnerabilities to see if they can gain access to the targeted devices. A person with a malicious intent can find information about vulnerabilities from one of the several organizational sites such as CVE (2004), Common Vulnerabilities and Exposures, or IAVA (2004), Information Assurance Vulnerability Alerts, that provide full disclosure. The hacker can then trace a vulnerability number from CVE to a source code clip on the public website such SecurityFocus (SecurityFocus, 2004) or via a general Internet search. He or she can then find corresponding detailed instructions on the exploit on the SANS (2004) or some other public website. This can all be done in minutes.

Most industry experts admit that a system or an environment of computer systems and networks that is hundred percent hacker-proof is yet to be invented. And, for the foreseeable future, IT users can best protect their assets by managing the evolving vulnerabilities that continue to threaten their environments (Masurkar, 2004). In spite of the the concerted efforts from many organizations, complete solutions are lagging behind. Traditionally, malicious code and backdoors (such as *rootkits*) and enabling vulnerabilities due to errors or negligence in system administration tasks caused exposures. In recent years, hackers have exploited multiple vulnerabilities at a time and have successfully launched multi-vector viruses.

These pose *blended threats*. It started with *Nimda* and *Code Red*, then *Slammer* and others, and, recently, *Blaster,* that caused widespread damage.

With the added advantage of knowing an organization's internal workings, insiders commit crimes that have been known to be on the rise for some time. This ability of malicious internal users to gain additional privileges on any system is not uncommon. Unfortunately, it is often overlooked by IT administrators and managers. What happens when an authorized user, such as an employee or a contractor working on the internal premises, turns malicious? She or he will gain access to another user's account through various possible means; via trusted relationship, poor password management, sessions left unlocked, to name a few. Once on a system, malicious users can use buffer overflow and other forms of attacks by compiling and executing exploit code available on the Internet to gain root privileges. Then the next step is to use a sniffer, install backdoors, maintain and gain additional access privileges using rootkits, and launch subsequent attacks.

Masurkar (2003) has compiled a list of worldwide organizations fighting security incidents. FIRST (2003) and CERTs from many countries continue to progress, yet struggle to coordinate the information regarding past incidents, trends and models to deal with modus operandi of attackers. To a vast majority of small to medium enterprises, the benefits don't seem as immediate. As against this, larger, multi-national enterprises can take advantage of CERTs. But these enterprises pose more ways to be vulnerable than smaller ones because of the multitudes of access methods into their intranets, DMZ servers, partner networks or Internet ASP sites.

As data centers have grown larger and more complex, upgrading hardware and software and managing security vulnerabilities has become a common tactic that regularly borders on strategy. What we mean is that due to the lack of any longer term solution IT organizations have a notion that, for the foreseeable future, it is an effective way to mitigate business risk. The same IT organizations, however, would not deny that it is an increasingly resource intensive tactic. Some vendors recommend patch management strategies (Radhakrishnan, 2003) to mitigate risks to critical assets by classifying business environments. Certainly, clients can benefit from this in deploying change management. But this doesn't solve the problem of segregation and analysis of massive amounts of security event data. Beyond segregation, the data also needs to be correlated so business decisions can be made to mitigate any perceived risk.

To help reduce cost and complexity, Managed Security Services providers (MSSP) sell user-friendly scalability management solutions (Outsourcing MSS, 2004) called *Managed Security Services* (MSS). More and more organisations are turning to MSSPs for a range of security services to reduce costs and to access skilled staff whose full-time job is security.

MSS-based vulnerability scanning matured in 2003, to be followed by intrusion detection in 2004, security monitoring and response in 2004, and authentication and administration by 2004 and 2005 (King, 2001). But the downside to all of this is that keeping up with the newer security devices and appliances and continuously developing attack signatures are daunting tasks for these vendors. Secondly, any organization relying on IT needs solid information security policies and practices. This is a challenge for many. Outsourcing components of information security should be evaluated as a solution, but the business must always retain responsibility, - thus underlining the importance of understanding business and regulatory implications of outsourcing security. Also, users examining managed security services should realize that multiple providers may be warranted, depending on the breadth of function outsourced. Lastly, in spite of the significant strides in recent years, customer-vendor trust (a factor that can be an issue for any service provider) remains a significant hurdle in delivering managed security services. This can slow down the fight against security incidents made affordable to some willing enterprises by the MSS business model.

There is a serious lack of training, awareness and standards across many IT organizations. Even if there is training provided in certain few ones, practitioners and technologists lack authority to make policy decisions. Aside from the global issue of *"digital divide"* that centers around the many poor and developing countries (such as in Africa) who are short on keeping up with the IT advancement, this lack of training, standards and authority has had a counter-effect on the fight against security attacks. It has not only encouraged negligence on the part of personnel who maintain information systems, but has promoted ad hoc approaches to incident response and change management. There are a few noteworthy efforts that address this issue. OCTAVE (2003) is one example. CERT-USA has introduced OCTAVE and its training, but OCTAVE as well as other such methodologies have yet to take hold in the industry.

3 FUTURE GLOBAL THREATS AND CHALLENGES

The global threats of the future are not simply from the hackers but also could come from international terrorists. Coordinated attacks are likely to be planned that may target power grids, nuclear reactors, water purification systems and other critical infrastructures that are the foundations of today's established societies. Secondly, the speed of the spreading of the attacks, such as viruses, will increase significantly. Dealing with high speed networks that are carriers of fast spreading viruses and worms, faster and massive scale coordinated attacks could be used as a weapon to bring quick

destruction. The Distributed DoS (DDoS) attacks prevented some of the biggest Internet vendors from functioning few years ago. That certainly sent a warning that, in the near future, the Internet could be a strong catalyst for even a bigger orchestrated crime.

Distributed intelligent, wearable (on-person) devices containing advanced sensing and communication capabilities hold promise for many societal benefits. But as these intelligent devices take hold, they will give rise to opportunities for miscreants to reenter, "camp out" or inject malware in ways unlike ever before (Duquenoy and Masurkar, 2004). Their ubiquity, mobility and ability to distribute information pose new challenges in the area of security, privacy and ethics. Extreme care is needed in designing them to prevent the malicious activities.

For many years to come, if we have to address Internet terrorism, increasing and highly efficient cooperation and communication between incident response teams will have to remain as a high priority for worldwide organizations such as United Nations that promote cooperation among nations. FIRST is currently carrying that responsibility, yet some aspects need progress. In particular, it is known that key incident information is not always conveyed effectively between response teams such as CERTs and incident response standards are lagging.

To a great extent, the information society can progress when IT security issues are adequately addressed. IT Security is one of the *eEurope 2005* initiative's six policy priorities. For supporting eEurope 2005 security policies, the European Network and Information Security Agency (2004) was set up to enhance the capability of the Community, the Member States and consequently the businesses to prevent, address and respond to computer security problems. It seeks to achieve an IT security culture within Europe. The tasks of ENISA will focus on advising the European Commission and the Member States on information security and in their dialogue with industry to address security-related problems, promote risk assessments research, deliver training and collaborate between public and private industries. How will ENISA maintain cooperation with the existing CERTs in some of the advanced European countries? And, with FIRST and CERTs across the world?

Survivability, in this context, is the ability of a computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner. Some research efforts are focused on establishing new methods for risk assessment and by developing engineering technologies for analysis and design of survivable systems as at CERT-USA (Ellison et al, 2002) . In spite of difficulties in funding, furthering the research efforts in threat and risk assessment is important. One group of researchers (Rathmell et al, 2000) claims that a deeper understanding of the potential threat actors, combining technical and psycho-social aspects, may

increase the probability of developing effective attack indicators. Thereby improving prospects for substantive warning before the threat materializes into a damaging incident. Such approaches require compilation of multi-source data (which needs to be up-to-date) and establishment of a monitoring regime limited to certain hacker groups and cyber-terrorists.

For any enterprise, meeting the legal and regulatory compliance is a necessary goal. To comply with the legislation and, when necessary, to make use of law to bring justice to computer criminals are difficult challenges. Obviously, legal activities can consume critical human and financial resources. Citizens' rights are sometimes overlooked when new laws come into play; so this is a serious consideration for the governments. In USA, for example, following the *"9/11"* disaster, the USA Patriot Act (2001) enacted by the President gives full authority to government agencies to investigate individuals without search warrants. Canada has also passed legislation following the events of 9/11; for example, Bill C-36, the Anti-terrorism Act, which received Royal Assent (2001). These laws can certainly help to swiftly investigate computer criminal activity, but are also seen by many citizens as the violation of their fundamental right to privacy.

Consider also that legal and technical personnel need to understand and be aware of each other's needs. Governments around the globe are continuously introducing stricter laws to protect the enterprise as well its clients and end users. So, here, the challenges lie in bringing the awareness and practical training of these laws and their implications to the incident response teams. Are there any simple answers to questions in any computer or Internet criminal case? For example: How to prosecute international computer criminals and bring them to justice?

4 ADEQUACIES OF LEGISLATIONS & REGULATIONS

Most industrial countries have computer crime legislation in place that are criminalising cyber attacks such as hacking, denial of service attacks or malware attacks. The question as to how much the computer criminal law can actually help to combat IT Misuse has been much debated (Brunnstein et al. 1995). It has also been a question of high interest for the IFIP working group 9.6/11.7, *"IT Misuse and the Law"*.

Computer criminal law could, alongside its criminalisation function, has perhaps the more important objective of acting as a deterrent. Besides, it can stand as an ethical marker and can have an educational function. However, it must be noted that, in general, criminal law is the strongest sanction available to states and carries considerable stigmatising effect. Hence, we should be careful not to extend this powerful approach to cases where its use

is unnecessary or inappropriate (Wasik, 1994). Secondly, hacking and malware-related crimes are often committed by young people that have social problems. They strive for attention and will hardly be deterred by legislation.

Problems in the prosecution of computer crimes arise because criminal acts are often either not detected or not reported by organisations which are concerned about the organisation's reputation. Furthermore, prosecutors (investigation officers, judges, and attorneys) are often lacking specific technical knowledge. Besides, detailed digital evidence or traces are often missing. In relation to the number of malware attacks, there have been only a few successful prosecutions of malware-related crimes. However, if there is no effective computer law enforcement in place that finally leads to punishment because just the computer crime laws by themselves can hardly have much of a deterrence and crime prevention function. Most computer crime legislations are implementing a general approach to regulate malware-related crime in which regulations are formulated to cater to a broad spectrum of criminal acts, including malware as a subset (e.g. offences against integrity of computer data and systems, computer sabotage).

Ten years ago, it had been discussed whether we needed new or improved laws to deal more aggressively with the virus threat. Some countries had introduced new regulations to apply specifically to various aspects of virus-related criminal acts, such as the generating, writing, promoting, offering, making available and circulating of viruses (e.g. Art. 144.2 Swiss Criminal Code). This specific approach to malware-related crime was enacted to fight the publishing of virus code or the selling of virus construction sets. However, today, malware is most effectively spread as worms, mass mailing viruses or via spam, and, consequently, distribution of virus code via publishing or selling plays an insignificant role.

Today, cyber attacks are usually trans-national computer crimes and an international cooperation and harmonisation of computer criminal law and regulations are necessary. The Cyber Crime Convention of the Council of Europe [CoE 2001], which was opened for signature in November 2001, is an important international instrument for combating trans-border cyber crimes. The CoE Conventions deals with cyber crimes directed against information and communication system, computer fraud and computer-forgery, copyright-related offences and content-related offences. It provides legal instruments for international cooperation and mutual assistance for fighting cyber crime.

On April 5, 2002, hackers accessed a California State payroll database containing sensitive personal financial information belonging to approximately 260,000 state employees. Legal and regulatory developments since the proposal of *SB 1386* became effective in July 2003 (California Senate Bill 1386, 2002). One of the primary motivations for many

companies is avoiding exposure to the uncapped civil action authorized by the law: *"Any customer injured by a violation of this title may institute a civil action to recover damages."* The law's intent is to alert people, whose personal data has been compromised to the danger of identity theft, in a timely way. But this is not enough. First, there needs to be a legislation at the U.S. federal level, and, secondly, other states need to follow California's lead.

There are more U.S. laws to comply with; HIPAA - Health Insurance Accountability and Portability Act (1996), GLBA - the Gramm-Leach-Bliley Act (1999), Sarbanes-Oxley Act (2002), to name a few prominent ones. These laws require enterprises to protect sensitive data such as customer records. Without compliance, companies may face heavy fine, bad publicity and other legal ramifications. According to these regulations, companies must identify, authorize and track user activities. Numerous other related laws exist; for example, USA Patriot Act of October 2001. Then there are Basel II, German KonTrag and others to discipline financial and risk management. They all must be kept in perspective and updated ,- which is a challenge for the law makers. But, also, this legislative burden is seen as overwhelming by most profit-oriented enterprises. So, the question comes up: how can governments promote legislation in the industry in a cooperative way?

An internationally harmonised approach is needed for fighting spam, which has become a major privacy and security problem. The EU has implemented a restrictive opt-in approach for regulating spam in the EU Directive on privacy in the electronic communication sector (EU-Directive, 2002), which disallows to send unsolicited emails to users unless they have given their prior consents or are in a customer relationship with the senders. However, under the U.S. Law, "CAN-SPAM Act" (2003), no prior permission is required for sending commercial messages as long as the receiver has the chance to "opt-out" of receiving future message from the same sender. It has been criticised that the U.S. legislation is not going far enough and could even make matters worse by approving spam that follows certain rules. Since approximately eighty percent of spam is believed to be sourced from North America, it is difficult to successfully fight spam in Europe if the U.S. legislation is following a weaker approach. The EU has called on the OECD (2004) to set up international efforts to fight spam. How can global security-aware communities help OECD to aggressively pursue this issue?

5 ORGANIZATIONAL DEFICIENCIES

Even though an organization may view a particular attack as its own problem, it is far more likely to be a piece of a larger puzzle. The attack in question is probably not aimed at that one particular (which is taken to mean corporation, academic institute or any other form of organization) but at achieving a certain goal, for instance enhancing the attacker's monetary situation. Phishing spam is an example where neither viewing the attack from the point of view of the account holder nor the monetary institute helps. Instead the entire picture needs to be taken into consideration. Global terrorism is an analogy here; the global threat cannot be dealt locally.

It was obvious right from the first major Internet incident, the Internet Worm, that coordinated incident response was needed. Therefore, CERTs were created at a per-organization and sometimes at country level to respond. To enhance the cooperation between these localized organizations, the FIRST was also founded of which many of the CERTs are members (FIRST, 2003). These help establish vital person-to-person contacts that can be useful in an emergency (Brownlee et al, 1998). However, is it enough? With so many fires to put out, shouldn't some of the communication be handled automatically and with automatic responses as was done in the Digital Immune System (Kephart et al, 1998)? For this to happen, the trust between the individuals would have to be extended to the mechanisms put in place. There may be legal issues to contend with too. On a technical level, even though the core protocols of the Internet are fairly robust, will that be enough to facilitate communication while the same network is under attack? Perhaps a back-channel network between CERTs would be on order that would allow automated alerts and responses.

The larger an organization's network grows, the more unmanageable it becomes. Even when the core network devices are well understood, the client and server machines are not. When an alert is registered for, say, an IDS system, claiming it has logged an attack package from one machine to another, it is not at all clear if the targeted the machine was vulnerable to the attack or not. Was the appropriate operating system, patch level or server software installed and active that displayed the exploitable vulnerability? Most exploit attacks are very finicky about the exact configuration of the target. Of course, the attack may not even have reached the target because it was filtered or dropped. So, the alert does not carry as much weight as one would like to think.

A good system administrator will want to pursue any likely alert, though. The next problem that faces him or her is tracking down the source and target machines in question. In the case of network devices, there exist usually plans of deployment that tell where these are geographically located and who owns them. Because these are often closed devices, with one set of

firmware (as opposed to an OS with various servers installed), it is easier to keep track of the software state they are in.

Servers are a bit more difficult. Server ownership may be more diverse, and their locations may not be confined to certain locations. A workgroup server may be set up in someone's office, for instance. The software state of these machines are also more complex to track, although usually servers are treated more conservatively than client machines.

Client machines, which are globally ubiquitous, are, of course, a nightmare. Apparently, to make administration easier, the DHCP protocol is used to assign IP addresses on demand. This is even the method of choice for fixed-location desktops in many organizations. Laptops are, of course, mobile by nature. They are taken into *'hostile'* environments and then back into the organization, possibly carrying malware of some sort. The IP address tells us little and the MAC address not much more as a laptop user may spontaneously decide to use a different network adapter. And, then there are the wireless roaming laptops that are allowed to keep their IP address even as they change location. So, tracking down a misbehaving laptop is not easy.

This organizational deficiency in terms of lack of self-awareness is problematic when trying to do risk analysis. In principle, we must update our exposure snapshot at every mutation of the network. That is an unlikely proposition. Then we would like to know how the current set of known vulnerabilities impact our given system and update this every time a new vulnerability becomes known. Also quite inconceivable.

Despite improvement in network management tools, and perhaps the recently more conservative spending on IT infrastructure, network management challenges have grown still faster. Instead of congealing on a limited set of architectures and software (which would be problematic for other reasons), the current trend is diversification, catalyzed by Java and Linux.

6 TECHNICAL EXPERTISE

Diversification also brings with it the problem of finding experts in these diverse fields who also understand security. Accreditation is of dubious benefit as it implies the field is stable enough to lay down in stone and test against. What is probably more important is a certain hacker mindset; however, with adult ethics packed in. But this can't be tested in any consistent way.

Size matters in converse ways. If an organization is too small, the few security experts may not have the resources between them to tackle all of the incident problems successfully. When an organization becomes too large,

the resources tend to get distributed which does not facilitate close cooperation. One possible solution is to outsource part of the security duties to a third party (such as the earlier mentioned MSS) that is both centralized and diversified enough to provide the qualified resources. Such specialized companies may also be then better able to attract (and retain) people of the right mindset to tackle difficult security problems. The danger is, of course, that they may not be able to pay enough attention to each individual organization when a global incident breaks that threatens all its clients. We could, however, argue that seeing the global picture may be beneficial to efficiency.

Harking back to the risk analysis discussion before, the consequences of a configuration change are probably not understood well by those making the decision. Even a security expert may have to research the consequences if he or she were asked beforehand. Security education must reach those that enable or implement features because very often simple changes can avoid a big exposure without much loss of functionality.

7 EDUCATION, RESEARCH, ADVANCED TRAINING AND INFORMATION RESOURCES

For the last decade, with the growing demand for secure systems and products, many universities have started to build up IT security research groups and to offer IT security courses or degree programs, particularly in the United States, Europe and in some specific advanced institutes in several parts of the world such as India and Israel. But how many of the current IT security curricula help develop expert knowledge needed for computer security incident analysis and response covering such areas as operating systems internals, intrusion detection systems, reverse engineering methods, computer forensics and methods of computer emergency response?

Europe is proposing a research effort to build a "Trusted Computing" platform, reminiscent of the TCPA (2004) initiative. Concerns have been raised, however, that an EU institution in this area could promote security by obscurity to the advantage of a few players.

In USA, there are several agencies of the federal government (e.g. NIST-National Institute of Standards and Technology) that are involved in research and creating guidelines related to the preventive as well as reactive side of security incidents. It is not clear how the federal guidelines will be adopted in the industry even though members of some of the major vendors partake in the development of the guidelines. Some of the agencies also fund universities to perform research or develop security education; for example, CERT-USA at Carnegie Mellon University or Purdue University. Among many efforts to inspire research in academia, there is the initiative to create

centers of academic excellence by the National Science Foundation in several universities for education in information assurance. In spite of this valiant effort, one can bring up an argument that currently, in the industry, matching jobs for such education may not exist in plenty in the near term, and that can be an issue for new recruits into the program or for graduating students.

Many training courses are offered to equip budding security experts. For those who already have some experience, security conferences offer a peek into potential problems and their defenses, and there are also specialized training events such as the Black Hat (2004) briefings. Little is known as to ultimately how successful such training actually is. With the right disposition, we can at least expect the trainee to know how to identify the right tools and go through the correct motions to handle an attack. Security incident response probably lends itself better to the apprenticeship model of training than the school house model because mindset cannot be taught by books.

It is also mandatory to stay up-to-date with the issues. There are mailing lists and information repositories for this purpose. BugTraq (2004), for instance, is a mailing-list where security risks are announced. Most people involved with security incident response keep track of such lists and a lot of important information is distributed through them. Vendors offer their own security advisories, but these only concern their own products. Security companies often have their own advisories, compiled from the vendors' advisories, other sources and their own research. Finally, some of the hacker groups publish their findings in different ways. Information glut is therefore a problem.

To distill the vast amount of information, various security bulletins are available that list the most recent threats. Some of these have the benefit of being translated into the native language of the reader so that the information can be absorbed more easily. Unfortunately, the publication cycle of such bulletins does not move as quickly as Internet time does, and the bulletins are often of little use by the time they reach the incident responder. A critical update may have been tragically delayed and an attack successfully launched.

The trend in updates is definitely going towards automatic updates in which a daemon periodically checks for new updates and installs them automatically. A lot of trust has to be placed in the creators of the patches to avoid mis-patching or introducing unwanted features. In the past, this trust has been occasionally misplaced (Knight, 2002). If the patch requires the restarting of software or the machine, the process may be inapplicable to mission-critical servers. The update distribution system should scale well and remain immune to the loss of one central server (as happened with a recent worm, which attacked the machine hosting the patches that prevented

its spread). However, on the whole, it is a worthy idea. Especially, for those vulnerable and difficult-to-locate client machines.

The security reports also have other problems. First of all, it is hard to tell how reliable the information is, as often the text is kept intentionally vague. It would be useful to have a ranking scheme (perhaps a la Amazon) whereby others can elevate or depress its importance. Even an important report on a Linux flaw will be irrelevant to a Solaris user. Often it gets more subtler than even that. Each report has to be studied carefully and then compared with the existing installation base to determine the risk. There have been bugs in code that related to a very large population of machines across architectures because they share the same design or code (NISCC, 2004). This would be made easier if the reports were well structured or at least well written. Of course, the intentional vagueness does not help, but there are circumstances when a report still needs to be used while there is no real fix or it is felt that hackers may profit from a detailed description. Often a more detailed write-up follows a more widespread disclosure of the problem. Even then, it is obvious that natural language is not the most precise form of expression for such information. Sometimes, the wording in ambiguous, or the objects not accurately described. And, often, write-ups are done by non-native speakers and much is lost in translation.

Some publications have more structure to them. CVE dictionary (which is not a database) brings some structure into vulnerability reporting and defines some of the terms. However, the description text is still free-form. In the field of alerts, the IETF (2004) has defined the IDMEF, the Intrusion Detection Message Exchange Format (Curry et al, 2004), and it is already much richer in vocabulary. And yet, much is still open to interpretation limiting the usefulness of it. Beyond an appropriate syntax, clear semantics are required to accurately describe a vulnerability or an alert. Building elaborate ontologies of all aspects of security seems the right path to take. However, it will be a very long and hard one and will probably never be perfect (Undercoffer et al, 2002; Debar et al, 1999).

Setting aside the complexities of building such an ontological framework for security incident communication, the holy grail for the responder will be the automatic risk assessment to his or her situation. Given all the possible problems that need dealing with, which one needs most attention?

8 PREPARATORY REQUIREMENTS

Contingency measures must be practiced or else they will not be effective. A backup is useless if it can't be restored. And often this means restored quickly. But before a machine can be restored, the effects of the attack should be analyzed with forensic tools so that all aspects of the attack

can be understood. Since all this has to be done under time pressure, the users of the tools must be trained.

Containment methods must be practiced and their impact on daily operations assessed. Can a single rogue machine be isolated by the incident response team quickly enough to prevent it from affecting other machines? Can network traffic be choked to prevent a worm from spreading too fast? In particular, worms need to be responded to in a matter of seconds to prevent widespread outbreaks.

Penetration testing is a useful method for probing one's defenses (Palmer, 2001). By putting oneself into the shoes of an attacker, the network takes on a different light and many faults become apparent. The question is, should this testing be done by an external team or internally? Certainly, an external team is likely to have more experience in the tools and tricks of the trade. However, the experience of trying the attacks is an important educational experience for the incident responders, and this is not something a lengthy report can replicate. Of course, once the penetration testing has been performed, one must ask if there are any lessons to be learned. Sometimes, the incident response team is not the same that sets the security policy and many problems remain unaddressed. However, if such a testing was performed internally, at least the experience will facilitate in maintaining the right mindset for dealing with real attacks.

9 CONCLUSION

In the present state, it is inexpensive, quick and easy to launch Internet or intranet attacks. However, for taking actions to effectively respond and prevent the security incidents the road ahead is tough. We need to harden our infrastructures, significantly improve global communication, cooperation and awareness, collaboratively fight hacking and terrorism, and perform cutting edge research such as in survivability engineering and threat assessment, and in setting standards.

The world's critical infrastructures and the government and business operations that rely on them are at serious risk. All nations should bear the responsibility to improve Internet security and help coordinate effective international global response to IT security incidents and events. In order to be successful, we need to ensure participation and cooperation among commercial enterprises, governments, law enforcement, security research organizations, and practitioners who can help further the art and deployment of incident response and prevention.

This paper summarized the current state as well as pointed out some key interdependent ideas that can help improve the overall capabilities.

However, as we pointed out, there are many open questions. The panel members intend to present these as only the starting points for discussion.

10 ACKNOWLEDGEMENTS

The authors wish to thank the following individuals for joining them in the discussion panel: Kai Rannenberg, Goethe University Frankfurt, Germany; Albin Zuccato, Karlstad University, Sweden; Gunnar Wenngren, Swedish Defense Research Agency, Sweden.

REFERENCES

Black Hat Briefings website, 2004, http://www.blackhat.org/

Brownlee, N., Guttman, E., "Expectations for Computer Security Incident Response", IETF RFC 2350, June 1988.

Brunnstein, K., Fischer-Hübner, S., "How far can the Criminal Law help to control IT Misuse?", International Yearbook of Law Computers and Technology, Volume 9, 1995.

BugTraq, http://www.securityfocus.com/

California Senate Bill 1386, 2002, http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

CAN-SPAM Act of 2003, "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", or the "CAN-SPAM Act of 2003", http://www.spamlaws.com/federal/108s877enrolled.pdf .

CoE - Council of Europe Cyber Crime Convention, 2001, http:// conventions.coe.int/Treaty/ en/Treaties/Html/185.htm.

CERT - Computer Emergency Response Team (2004), http://www.cert. org/

CVE - Common Vulnerabilities and Exposures (2004), http://cve.mitre. org/

Canadian Government's Bill C-36, http://www.parl.gc.ca/37/2/parlbus/ chambus/house/ bills/summaries/C17-e.pdf

Curry,D., Debar, H., Feinstein, B., "The Intrusion Detection Message Exchange Format", IETF, 2004 http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-11.txt

Debar, H., "Towards a taxonomy of intrusion-detection systems", Computer Networks, 1999.

Duquenoy, P., Masurkar, V., "Surrounded by Intelligence", in Risks and Challenges of the Networked Society. Proceedings of 2nd IFIP Summer School, 2003. (Forthcoming)

Ellison, R., Lipson, H., Linger, R., Mead, N., Moore, A., "Foundations for Survivable Systems Engineering", CrossTalk, The Journal of Defense Software Engineering, July, 2002.

ENISA, European Network and Information Security Agency, http://www.ffii.org/proj/enisa/index.en.html

European Commission's (EU) Directive on Data Protection (1999). http://europa.eu.int/comm/internal_market/privacy/index_en.htm

EU Directive 2002 - DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

FIRST Operational Framework, http://www.first.org/about/op_frame/ op_frame. 20030627.html, 2003.

GLBA – Gramm-Leach-Bliley Act (1999). http://www.ftc.gov/privacy /glbact/

HIPAA - Health Insurance Portability and Accountability Act (1996). http://www.hhs.gov/ocr/hipaa/privacy.html

Information Assurance Vulnerability Alerts (2004). http://www.iava.org/

IETF – Internet Engineering task Force, http://www.ietf.org/

IFIP Working Group, - IT Misuse and the Law, http://

Kephart, J., Sorkin, G., Swimmer, M., White, S., "Artificial Immune Systems and Their Applications", Springer, 1998.

King, C. "META Report: Are Managed Security Services Ready for Prime Time?" INT Media Group. July 13, 2001, http://itmanagement.earthweb.com/secu/article/ 0,,11953_801181,00.html.

Knight, W., "Microsoft's anti-piracy plans spark controversy", New Scientist, July, 2002.

Masurkar, V., "Responding to Customer's Security Incidents, Part 3: Following Up", Sun Blueprints Online, September, 2003, http://www.sun.com/solutions/blueprints/0903/817-3733.pdf

Masurkar, V., "On Developing a Methodology for Managing Security Vulnerabilities", Information Institute's 3rd Security Conference, April, 2004.

Nessus Remote Security Scanner, 2004, http://www.nessus.org/

NISCC, 2004, "Vulnerability issues in TCP", http://www.uniras.gov .uk/vuls/2004/236929/index.htm

Nmap Security Scanner, 2004.,http://www.insecure.org/nmap/

OCTAVE Methodoloy (2003). http://www.cert.org/octave/

OECD- Organization for Economic Cooperation and Development, http://www.oecd.org/

Outsourcing Managed Security Sources, http://www.cert.org/security-improvement/ modules/omss/b.html

Palmer, C., "Ethical Hacking", IBM Systems Journal, 2001.

Radhakrishnan, R. (2003). A Patch Management Strategy for the Solaris Operating Environment, Sun BluePrints Online, http://www.sun.com/ blueprints, January 2003.

Rathmell, A., Dorschner, J., Knights, M., Watkins, L., "Early Warning & Threat Assessment for Information Assurance", RAID 2000 Proceedings, October, 2000.

SANS Website, 2004, http://www.sans.org/

Sarbanes-Oxley Act, 2002, http://www.sec.gov/spotlight/sarbanes-oxley.htm

SecurityFocus Website (2004), http://www.securityfocus.com/

Spafford, E., "The Internet worm program: An analysis", CSD-TR-823, Purdue University, 1988.

TCPA - Trusted Computing Platform Alliance, 2004, http:// www.trustedcomputing. org/home/

Undercoffer, J., Pinkston, J., "Modeling Computer Attacks: A Target-Centric Ontology for Intrusion Detection", RAID 2002 Conference Proceedings, October, 2002.

USA Patriot Act of 2001, http://www.epic.org/privacy/terrorism/ hr3162.html

Wasik, M., "Foreword in Security and Control of IT in Society", edited by Sizer, R., Yngström, L., Kaspersen, H., and Fischer-Hübner, S., North-Holland, 1994.

West-Brown, M., Kossakowski, K., "International Infrastructure for Global Security Incident response", CERT-USA Report, SEI, CMU, June, 1999.