KPMG

# E-COMMERCE AND CYBER CRIME:

## New Strategies for Managing the Risks of Exploitation

FORENSIC AND LITIGATION SERVICES

*"Now that most transactions and exchanges have become electronic, you really don't need to be an expert to predict that this will become, or already is, a crime generator. What is relatively new is the value of business information. We see a tendency for rising criminal activity in this field. Not only the theft of information, but also the threat of making information public."*[1]

Loek Weerd, Police Inspector and Computer Crime-unit Expert,
Haaglanden Regional Police, The Netherlands

## TABLE OF CONTENTS




*Produced as part of a series by KPMG's Assurance & Advisory Services Center.*

At the turn of the millennium, one would be hard-pressed to find a competitive and thriving organisation that does not rely upon communications and other information technologies as an enabler of its activities. No longer incidental to the workings of an organisation, technology is integral to business today. At the same time, however, the very "digital nervous system,"[2] as Bill Gates terms it, that enables and improves our lives at work and at home also creates enormous new risks, many of which organisations may not perceive or have not yet considered.

The complexity of modern enterprises, their reliance on technology, and the heightened interconnectivity among organisations that is both a result and a driver of e-business—these are rapidly evolving developments that create widespread opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organisation. With the growth of e-business, internal and external perpetrators can exploit *traditional* vulnerabilities in seconds. They can also take advantage of *new* weaknesses—in the software and hardware architectures that now form the backbone of most organisations. In a networked environment, such crimes can be committed on a global basis from almost any location in the world,[3] and they can significantly affect an organisation's overall well-being.

As businesses grow and partner, systems become increasingly sophisticated and less dependent on human intervention. Monitoring individual behaviour becomes more difficult (though certainly more important); and vulnerability to electronic crime grows as organisations are increasingly connected to, and reliant on, individuals and systems they do not directly control. Most organisations are alert to the risks posed by electronic viruses such as the May 2000 "I Love You" virus, which spawned a number of derivative viruses and is estimated to have cost businesses and governments upward of $10 billion

dollars.[4] Many, however, remain unaware of the extent to which they can be harmed by a wide variety of cyber misbehaviour that may originate with their own employees or partners.

As organisations develop and refine their e-business strategies, they need to consider the issues that influence the confidentiality, integrity, and availability of their data. In this context, they need to know how they can be affected by the new risks of e-crime and how inadequate preparation could leave them open to an attack that could easily diminish the value of their businesses.

***This white paper focuses on how organisations can use a comprehensive cyber defence program to turn e-crime preparedness into a new competitive advantage.***

This white paper focuses on how organisations can use a comprehensive cyber defence program to turn e-crime preparedness into a new competitive advantage. It describes the business risks now evolving rapidly in the electronic marketplace. It discusses how some attacks take place as well as how some organisations are beginning to protect themselves, both to deter and respond to attacks and to avert further damage once an exploitation has taken place. Finally, this document examines how the scope and nature of e-crime is expected to change and how organisations can prepare to meet those new challenges.

Increasingly, organisations are incorporating technologies into their infrastructures without understanding how such tools can be exploited and used against them—at a heavy price. Attackers can divert financial assets, shut down communications among employees or business partners, steal intellectual property, damage an organisation's reputation, or bring e-commerce (or an entire business) to a halt. Computers can be used as weapons to commit crimes, as storage devices to harbour evidence of crimes, and they can even be the objects or victims of crimes.

As organisations increasingly integrate their systems with those of their vendors, suppliers, customers, and others, the risks they face multiply. The shift toward "self-service" systems within and among organisations—capabilities that offer enormous opportunities for cost savings and other efficiencies in, for example, human resources, inventory, or billing—also makes their host organisations increasingly vulnerable.

Along with Internet use (projected to encompass 502 million users world-wide by 2003[5]), the e-crime problem is exploding: "A recent survey of Fortune 500 companies by the FBI and the Computer Security Institute found financial losses from computer crime exceeding $360 million from 1997 to 1999. Of those responding to the survey, 62 percent reported computer security breaches within the last year."[6] These numbers, however, do not entirely capture the nature or potential extent of the problem, as described by U.S. Deputy Attorney General Eric Holder:

> *How big is the computer and high-tech crime problem? We simply don't know. We do know that computer crime costs industry and society billions of dollars every year. There is substantial evidence computer crime is increasing in scope and in complexity. And we know that, left unchallenged, computer crime will stifle the expansion of electronic commerce and, potentially, pose a serious threat to public health and*

*safety, particularly when we look at the vulnerability of critical infrastructures, such as the air traffic control system, the power grid, and national defence systems—all of which are totally dependent on computer networks.*[7]

Such attacks are possible in part because the Internet and its related suite of communication protocols were designed (30 years ago) to facilitate a ubiquitous information-sharing and messaging infrastructure. Intended to provide continuity of communications services under wartime conditions, these protocols were never designed to be secure from exploitation. Although the characteristic strengths of the Internet served its initial purpose well, those same strengths embody features that are exploitable. Moreover, new technologies are being developed so quickly that all security issues may not be addressed completely during the development process.

***Organisations may not perceive the extent to which they can benefit from preparedness efforts.***

Apart from inherent technological weaknesses is the lack of e-crime awareness among many organisations. Many do not realise that the same technological advancements that have enabled business growth and innovation are also available to facilitate cyber misbehaviour. In addition, organisations may not yet understand that protecting assets in the virtual world is a more complex and exacting endeavour than protecting assets in the physical world. Organisations may not perceive the extent to which they can benefit from preparedness efforts.

### Recognising Your Attacker

Popular misperceptions often attribute network attacks to mischievous teenagers or social misfits. Experience indicates that these individuals, however, represent a small number of the diverse group of criminals who perpetrate e-crimes both inside and outside organisations. These criminals may commission e-crimes for their own objectives or make their skills and services available for hire.

External intruders include:

- Sophisticated "crackers" who—working alone or with trusted associates and sometimes for hire—develop and use technology-based tools that facilitate illegal entry into a victim's network system or other technologies. Once they have achieved their objectives, they distribute their tools anonymously, via the Internet, to mask their association with either the tools or the exploitation of the victim.
- "Cookbook" crackers[8] who lack the knowledge, skills, and abilities to create and use sophisticated intrusion tools but who seek out such tools to launch attacks.

Internal attackers can include dissatisfied current employees working alone or with other insiders or perhaps with disgruntled ex-employees. Some experts believe that organisations face a greater risk from the fraudulent acts of their own employees (or former employees with knowledge of their systems) than they do from external threats.[9] Contractors or employees of suppliers or vendors who exceed their authorised use of an organisation's systems also pose a considerable threat.

### Attackers Share Motivations

No matter who perpetrates it, a deliberate cyber attack can:

- destroy an asset (in which case, it retains no value),
- corrupt an asset (reducing its value),
- deny access to an asset (which still exists, but is unattainable), or
- result in the theft of an asset (which retains inherent value, but its possession changes).

Greed, malevolence, revenge, or the misguided intellectual challenge of creating havoc within large systems can motivate both outsiders and insiders. External attacks involve outside offenders breaking into a victim's network either to take something of value[10] or for the purpose of "trojanising" the network. (Named for the Trojan Horse, this crime is that of compromising network security measures and modifying security tracking mechanisms or legitimate programs to permit future unmonitored access. The perpetrator's purpose is to gain complete control of a victim's system so as to be able to execute unauthorised functions unknown to the owner or host of the system.) For example:

***Internal and external attackers share similar motivations: greed, malevolence, revenge, or the misguided intellectual challenge of creating havoc within large systems.***

- "The developer of a highly rated e-commerce shopping cart is accused of building a software backdoor into the program that could give him or hackers complete control of the server on which it's installed. The Dansie Shopping Cart, which is currently in use at more than 200 e-commerce sites and is recommended by several Web hosting firms, contains code that enables the author…to potentially run any command on the Web server."[11]
- In another case, "A Delaware man was found guilty in federal court [on May 16, 2000] of setting off a computer 'time bomb' that halted manufacturing by a high-tech company, causing $10 million in losses, the U.S. attorney's office for New Jersey said. A U.S. District Court jury in Newark found [the individual] guilty of unlawfully transmitting a program or command that resulted in intentionally caused damage to a protected computer. He had been charged under the four-year-old National Information Infrastructure Protection Act."[12]

Internal attacks are perpetrated by employees or trusted associates who exceed their authorised access to the organisation's systems and facilities. For example:

- "Recently, Internet Trading Technologies Corporation in New York suffered hacking activity…by an employee. The disruption to [its] business lasted for three days and had the potential of affecting a large percentage of Nasdaq trades conducted by the company. Fortunately, the employee did not employ a sophisticated attack and was traced. He was charged with sending data to intentionally cause damage to a computer, punishable by five years in jail."[13]
- As organisations might expect, disgruntled former employees can also wreak havoc. Recently, "Three Internet-only radio stations have gone off the air after they were actually removed from the computer server they were hosted on by a 'disgruntled former employee.' The three electronic music stations, E101, Pro G, and Trance Invasion, are operated by EbandMedia—a start-up company owned by Internet incubator iWeb Corp."[14]

Denial-of-service attacks (including those of offenders who launch viruses) can be perpetrated internally or externally to disable network and e-commerce services. A number of high profile attackers have been successful recently in their assaults on popular e-commerce firms including Yahoo, Amazon, and eBay. These attacks use the large-scale communications bandwidth of an intermediary to overwhelm their victims' systems with meaningless service requests, thereby degrading or denying legitimate users any service.

### How Organisations Become Victims

Intruders "case" their targets just as other criminals do.[15] They use publicly available information about the technical vulnerabilities of network systems coupled with inside information gathered from unwitting persons[16] to develop attack methods. Both external and internal intruders look for easy-to-exploit weaknesses in their targeted systems or facilities to gain illegal access to them. With the help of specifically trained professionals, organisations can take steps to protect against such vulnerabilities, as outlined in *Figure 1* on page 8.

However, not all attacks begin in cyberspace. Indeed, the physical security of systems and facilities is vital to a proper cyber defence program. (In fact, a fire in an ill-designed facility is as effective, if not more so, in shutting a facility down than, for example, a denial-of-service attack.) Organisations need to ensure that their physical security systems appropriately control and monitor the comings and goings at their facilities to prevent, for example, an attacker posing as a vendor or service provider from installing unauthorised software on a server to facilitate a subsequent intrusion.

**Figure 1: Guarding Against Common Risks**

| Attackers look for... | How it creates a weakness | How to mitigate this risk |
|---|---|---|
| ...network computer operating systems, workstations, and other devices deployed in "default" configurations. | A device in a "default configuration" is one that has had little or no reconfiguration to customise it after it left the manufacturer—a frequent practice that provides crackers with a quick and easy way in. | Turn off unneeded services that run by default upon installation on network servers, and ensure that all servers operate with up-to-date security patches to limit exploitation. |
| ..."misconfiguration" of hardware or software, perhaps by activating network services, such as FTP, that have known security issues. | FTP can be used to transfer large amounts of information off of or onto a system. Many FTP server applications have weaknesses that are well known and can be exploited during an attack if they are inappropriately configured. | Design and implement rigorous product selection and testing procedures. |
| ...a "one-size-fits-all" approach to cyber network defence (such as a software-based firewall). | Demonstrates a limited conceptual approach to the complexities of cyber network defence. | Conduct an enterprise-wide architectural security assessment of the domain; create and implement forensic incident response guidelines. |

## Partnering Also Creates Vulnerabilities

Businesses often outsource desktop and other Internet-based network support services. Most are also developing e-business alliances and other partnerships with customers, suppliers, and employees—relationships that are essential to e-business. Improperly managed and controlled, however, these new relationships can be as problematic as they are beneficial because, by their very nature, they entrust partial and sometimes complete control of the enterprise's information assets to an outside party.

To verify the professional qualifications and integrity of third-party service providers or potential partners, organisations should consider issues including:

- What individuals and entities have ownership interests in the service provider or potential partner?
- Is the provider/partner owned or controlled by foreign interests (outside of the host nation)?
- What is the cyber security infrastructure of the provider/partner?
- In what country are the servers of the provider/partner located (and what are the legal issues associated with that location/jurisdiction)?
- What personnel vetting procedures does the provider/partner follow before hiring and exposing its employees to client environments?
- Does the provider/partner have contract oversight clauses and an oversight apparatus in place?

### Dealing with the Consequences

Direct loss of assets is just one consequence of cyber misbehaviour. Whether the attack comes from inside or outside the organisation, victims often suffer from negative publicity, which can harm the organisation's brand and reputation, erode relationships with customers and other stakeholders, and eat into potential revenue. In fact, a March 2000 survey conducted by the Gallup organisation for At Plan, an online marketing firm, suggests that consumer confidence in online shopping has been hurt by attacks on prominent sites:

> *A third of online consumers overall said they might be less likely to make a purchase via the World Wide Web in light of recent news events…Nearly seven in 10 online shoppers contacted in the telephone poll said they were concerned or very concerned by news of attacks that had blocked access to such Web sites as Yahoo and Amazon.*[17]

This ever-present array of threats underscores the growing need for organisations to develop a cyber defence program that weaves preventive measures into the fabric of e-business operations. Along with a strong emphasis on prevention, a cyber defence program must also focus on detection—in the form of a sound forensic incident response process. Such a process establishes policies and procedures for departmental and individual behaviour and encompasses plans for ongoing communication with employees and other stakeholders, analysts, and the press.

Such an incident response process cannot be geared simply to the occasional emergency. Organisations repel numerous attacks each day. Such assaults are part of doing business in an interconnected world, and not every one should be treated as a crisis. Leaders need to be judicious in determining how to respond to various attacks, remembering that attempted "hacks" are as illegal as successful ones, and their perpetrators can be charged with attempted crimes. In emergency situations, the critical issue is to preserve the forensic evidence that will assist in identifying, apprehending, and prosecuting the perpetrator(s), as discussed in the next section.

**Remediation or Investigation?**

This is the continuing question for victims of network system intrusions. Many victims mistakenly believe that they prevent future intrusions by disregarding an exploitation, reinstalling network operating system software, and continuing with business. Ignoring the problem in this way, however, does not solve it or prevent future attacks. Criteria to remediate or investigate should be included in forensic response plans.

### Tools of the Intruders' Trade

Electronic criminals commit their crimes using a wide variety of easily accessible tools that are often available free on the Internet. Such tools include:

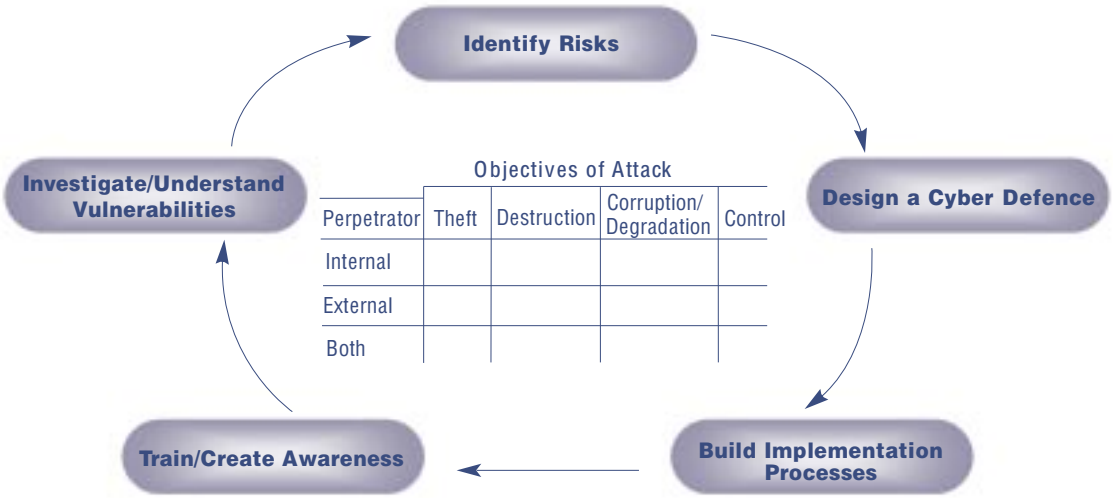
- Anonymous re-mailers: Machines on the Internet configured to receive and re-send traffic by replacing the original source address of the sender with the address of the anonymous re-mailer machine. Used by intruders to mask their identities.
- Internet packet filters or "sniffers:" Software that allows intruders to intercept network traffic.
- Nukers: Software tools used by intruders to destroy system log trails.
- Password crackers: Software that allows intruders to "break" encrypted password files stolen from a victim's network server.
- Scanners: Automated software that helps intruders identify services running on network machines that might be exploited.
- Spoofers: Software tools that allow intruders to masquerade as other users.
- Steganography: A method of encrypting and hiding data in graphics or audio files. Used by intruders to spy, steal, or traffic in information via electronic dead drops, for example, in Web pages.
- Trojan programs: A legitimate program altered by the injection of unauthorised code into that program causing it to perform unknown (and hidden) functions to the legitimate user/system owner. Intruders use them to create undocumented "backdoors" into network systems.

E-business security is an ongoing, comprehensive process of adding, removing, and managing layers of actions based upon holistic risk management strategies. In military and other organisations, this concept is now referred to as "defence in depth," a popular moniker that does not capture sufficiently the concept of a "from-the-inside-out" cyber defence.

***Increased access increases vulnerabilities: a cyber defence must encompass all points of interconnectedness, from the inside out.***

Because organisations are providing greater access to their systems to both people and systems outside their direct control, they must integrate a cyber defence that encompasses all points of interconnectedness, from the inside out. If they fail to do so, they may leave themselves vulnerable to attacks via, for example, a trusted supplier. Automotive and electronics manufacturers among others, for example, commonly use inventory management

**Figure 2: Helping to Ensure Preparedness**



systems that make information available to vendors, who then automatically replenish inventory supplies in accordance with established service-level agreements. These systems offer organisations untold benefits—and also pose innumerable risks. Should an attacker gain access to such a system and alter a manufacturer's request for parts in a manner that appears authentic to the vendor, an assembly line can grind to a halt. A cyber defence system must be designed to protect against these and other problems of interconnectedness.

Many organisations, however, have not adapted their security strategies to the inter-connectedness of the electronic world; consequently, they tend to think about security and risk management solutions in a disjointed fashion. They may rely on limited or "one-size-fits-all" strategies such as a particular brand of firewall or a specific means of controlling users or modem deployment. They may favour hardware and software solutions from particular vendors, or take the advice of vendors with whom they have an established relationship in one arena but who may not be qualified to help them with the highly technical specifics of e-crime preparedness.

In the face of escalating e-crime risks, organisations need to avoid one-dimensional, under-informed behaviour and, instead, develop a holistic strategy for a cyber defence (see *Figure 2* on page 11).

Leading organisations:

- establish clear, focused, integrated security policies
- provide employees with appropriate awareness and technical training
- hire capable, trained workers and support them in establishing and maintaining an integrated response to attacks
- instill awareness of electronic threats and risks throughout the organisation
- pursue the perpetrators of e-crimes against the organisation to the fullest extent of the law

Such a system offers innumerable benefits both in helping to deter attacks and in diminishing the effects of an intrusion, should one occur. Properly implemented and communicated, an enterprise-wide cyber defence system can help the organisation prevent liability on behalf of client management, avert potential lawsuits or regulatory action, recover lost revenue, and maintain or restore its reputation and integrity. Preparedness can, thus, become a strategic advantage in a business environment increasingly dependent on the security and reliability of computer networks.

## A Good Offence Is the Best Defence

An enterprise-wide cyber defence ideally includes integrated strategies, established in the form of philosophies, policies, procedures, and practices, and implemented through defined action plans. Such strategies should encompass technical, legal, and business strategies and they should be implemented in a way that considers employees, customers, suppliers, third-party relationships, and other key stakeholders. Thus, rather than a "wrap-around" capability encompassing systems and processes, a strong cyber defence is an integral part of those systems and processes.

In creating a cyber defence, organisational leaders should consider carefully what they have to lose. New-economy business assets encompass a wide variety of intangibles that can be removed with ease in a virtual setting. To understand the implications of potential losses—and to be able to defend against them—organisational leaders need to learn to define "assets" in the widest possible way.

**Assets that could be lost through electronic crime include:**

- banking and financial transactions data
- information related to a business' competitive position
- command and control system data for satellite systems and aircraft
- intellectual property (processes, methods, trade secrets, proprietary data, and other intangible assets)
- litigation-sensitive documents
- personal identification data (whose loss can lead to "identity theft" or stalking)

Once organisations know what they need to protect, they need to develop a strategy for implementing an enterprise-wide defence program. Such a strategy must encompass response procedures and standards that are integrated into day-to-day business operations. Cyber defence plans should strike a balance between the demands of accountability of business interests and the privacy interests of employees and customers. The concepts of openness versus security should also be considered in the context of a global electronic environment.

Leaders need to be sure that their business processes accommodate and facilitate a cyber defence. They should also ensure that they have configured the technical architecture of their systems in a manner that complies with and supports the cyber defence architecture. (How they set up and configure how particular transactions will take place, for example, must be consistent with the cyber defence program.) In addition, leaders need to communicate the purpose and value of their cyber defence and assign specific roles and responsibilities for carrying it out. Such a defence plan would encompass:

***Enterprise-wide planning***

- development of a cyber defence infrastructure
- integration of human and technical solutions into plans
- design and implementation of electronic network intrusion response plans
- design and implementation of network monitoring and management plans

*Enterprise-wide policy development and implementation*

- use of non-disclosure agreements governing trade secrets, standards of professional conduct for employees, and related issues
- policies governing the use of communication systems
- policies and action plans to assess the risks as well as the benefits of outsourcing with business partners
- policies and action plans tied to assessments of potential civil liability

*Training programs on e-crime threat awareness*

- incident response training for all employees
- incident response and security training for systems administrators and other technical service personnel
- creation and maintenance of forensic incident response guidelines
- inclusion of legal and policy issues in annual ethics training sessions for all employees

**A Business Leader's E-Crime Checklist**

Most organisational leaders are familiar with the traditional red flags that could indicate the existence of internal crime. However, e-commerce has changed the shape of business, including the nature and scope of risks. Here are 10 critical questions to help assess how your organisation may be at risk for e-crime:

1. Do you have policies and procedures in place for forensic incident response, privacy, and customer management (to mitigate civil exposure)?
2. Do you have a plan in place for communicating these policies effectively?
3. Do you have effective training programs for personnel at a variety of levels, encompassing cyber threat awareness and forensic incident response?
4. Do you have methods in place for vetting potential outsourcing providers?
5. Do you ensure that third-party sources for sensitive technology support are properly vetted as well?
6. Do you perform penetration tests of network systems to correct vulnerabilities?
7. Do you take specific steps to ensure the security of network servers or other systems where intellectual property or other sensitive data are stored?
8. Do you run network intrusion detection systems regularly and have an established plan for following up on the results?
9. Do you run logging functions to record evidence of irregular activities?
10. Do you monitor those network systems on which you deploy banners?

When an exploitation occurs, failure to respond or investigate may expose the enterprise and its directors, management, and shareholders to legal and operational risks. Yet, experience shows that many organisations, their employees, lawyers, and technical advisers have little or no understanding or experience in dealing with threatening cyber events. Unintentionally, they often underestimate the intrusion and then fail to take actions that would deter further losses. In other cases, they inadvertently destroy the digital evidence needed to support prosecution, civil litigation, or to provide a basis for administrative action.

Organisations can lose assets in nanoseconds through electronic crimes. When leaders believe that a crime has occurred, they must react instantly, following established forensic incident response plans to minimise further losses, assess monetary and programmatic damages, affix responsibility, and try to recoup losses. The response should include efforts to minimise the organisation's civil exposure. To implement such a plan, however, demands an integrated response to the range of legal, technical, programmatic, business, operational, and other issues that are affected by cyber misbehaviour.

***How organisations deal with an intrusion can help mitigate—or exacerbate—its effects.***

### Response Personnel Must Have Specific Skills

Today's business leaders recognise the demand for skill sets in the information technology (IT) field. In general, however, IT professionals are trained to set up and provide specific technology services. Typically, they are neither trained nor experienced in dealing with exploitations of those technologies. IT security professionals focus on constructing defensive measures to deal with threats, and some of them are experienced in understanding exploitations. However, very few IT security professionals have the experience and authentic forensic backgrounds to effectively investigate and gather evidence of network-based cyber crimes to be used during the ensuing litigation process.

Cyber investigators must have extensive hands-on experience with and knowledge of computer networks, programs, operating systems, and monitoring tools and practices. Moreover, they must be trained and experienced in the art of the collecting, examining, analysing, and reporting digital findings via a painstaking forensic process to render the evidence admissible in court. Beyond their network and forensics capabilities, investigators must also be skillful at interviewing, knowledgeable about legal issues in various world-wide jurisdictions, and aware of personnel law. They should also be able to act as expert witnesses and interact with the media, should the investigation require it (see *Figure 3* below).[18]

When responding to attacks, inexperience and lack of knowledge cause businesses to make mistakes that could easily be avoided—and can be devastating in their cost. They include:

- allowing untrained personnel to destroy evidence through inappropriate investigations
- failing to control information during and after incident detection and response implementation
- writing damage assessment reports that inadvertently mitigate losses in favour of the intruder
- using "honey traps," "ruses," and other intelligence-gathering methods in ways that fail to protect the respective parties' rights or inadvertently allow an attacker to use the defence of entrapment
- misinterpreting criminal laws by failing to seek appropriate counsel

**Figure 3: Digital Forensics—The Recovery of Evidence**

### The New Risks of Civil Litigation Exposure

The use of the Internet as a medium for the conduct of business also poses the risk of civil litigation exposure. The question has become, to what extent is an organisation liable for the consequence of damages caused across communications networks by the exploitation or pirating of its point of presence on the Internet? The answer depends on whether the entity exercised "cyber vetting" in developing and implementing appropriate measures to mitigate the risk of cyber misbehaviour.

To mitigate civil risks, organisations need to be able to demonstrate that they have developed and implemented adequate policies and reasonable cyber defence measures. Simply put, they need to take appropriate steps to help ensure that their facilities are not used to harm others.

### Legal Systems Lag Behind Technology

Another issue for organisations world-wide is the extent to which cyber crime laws—and perceptions about what constitutes, for example, hacking or other illegal behaviour—vary widely across borders. Forensics experts must be knowledgeable about the rules and limitations in each jurisdiction that may be involved in a particular incident.

In many jurisdictions outside the U.S., however, laws lack the reciprocity that all nation states need to protect their interests and those of their citizens. As U.S. Attorney General Janet Reno noted recently,

> *…If France is investigating a French businessman who never set foot out of France and all his records are stored on his computer and if France gets our equivalent of a search warrant for that computer, but the French businessman who is under investigation happens to be a customer of America Online and the records are stored here in Dulles in the United States, does the French order reach to Dulles?…*[19]

Clearly, e-commerce business and consumer issues driven by trans-border cyber incidents and the need for nation state reciprocity will drive the need to harmonise international approaches to cyber laws (see *Appendix I*).

International protocols are in development; but some experts believe that the seamlessness of the Internet may always require that disputes be resolved on a case-by-case basis. In this uncertain environment, business leaders must be all the more assiduous in working to secure their systems and protect them against further damage if an attack does occur. They must take particular care to

understand the relevant laws that apply in the countries in which their servers are located. In addition, leaders must take steps to understand how content providers, service providers (other than hosting companies), and the organisation itself could be legally implicated in a forensics situation. They must be aware of the courses of action available should a content (or other) provider's system be used to compromise that of their own organisation.

With the passing of the immediate threat posed by Y2K, the public and private sectors have begun to focus on cyber network defence. Leaders perceive that as technology changes, risks will also change. New technologies will pose new risks and demand new responses to those risks.

In the future, for example, new technologies such as holographic memory, nanotechnology (atomic- and subatomic-level structures), new communications protocols, and other technologies will be introduced and embedded into new core products that organisations will use to facilitate productivity in their infrastructures. Detecting exploitations of these technologies will remain outside the core mission of many organisations—but will require the heightened focus of all organisations. Issues related to the protection and storing of intellectual property developed in a network environment will also create concerns, and cyber protection methodologies will be paramount in this context.

***As the technology continues to change, organisations must take steps to understand the related risks that will evolve with technology.***

As the technology continues to change, organisations must take steps to understand the related risks that will evolve with technology. They must understand how they might be affected by those risks and ensure that their cyber defence processes and controls are continually updated to meet evolving needs.

The explosive growth of Internet-based open networks paves the way for instantaneous and devastating trans-national electronic crimes that can deny victims the ability to operate their businesses or control their assets. These exploitations will multiply as technologies change, as new technologies are introduced, and as intruders' methods inevitably become more sophisticated. Indeed, cyber crime will remain a fact of life for organisations everywhere.

As a result, organisational leaders must take specific steps to defend their assets against electronic crimes with a comprehensive program of training and cyber defence preparedness (see *Figure 4* below). They must also establish a plan for how they will respond should an intrusion take place. (Such a plan offers a wide array of benefits, not the least of which is that it can help enable a successful recovery as well as an effective prosecution of the offenders.) Properly implemented, an integrated program for mitigating the risks of cyber misbehaviour can also become a strategic advantage in a world increasingly dependent on the security and reliability of communications networks.

**Figure 4: Promoting Organisational Preparedness is a Continuous Process**

# Appendix I: Ensuring Preparedness — An Interview with Jeff Hormann of AARP

*Jeffrey S. Hormann is the manager of information systems security at AARP, a non-profit, non-partisan association dedicated to shaping and enriching the experience of ageing for its 30 million members. In this new role, Hormann is responsible for developing, implementing, training, and managing all aspects of information security within AARP's $40 million annual IT program. Before joining AARP, in February 2000, Hormann served 19 of his 22-year Army career as a criminal investigator, in which role he developed a comprehensive, Army-wide computer crime program from which emerged the Army's first and only organisation dedicated to investigating computer crime.*

*Below, Hormann discusses the importance of a comprehensive cyber defence program that has the collective involvement of all organisational members as well as the formal commitment of top management.*[20]

**Today's organisations are more dependent than ever on technology—which makes them vulnerable even as it offers great benefits. What are the main risks that organisations face as a result of their increasing reliance on technology?**

No matter how advanced the technology, the biggest risk is always going to be the human factor—whether it's the external hacker trying to get in, or a poorly trained or overworked system administrator who improperly configures the system, or—probably the greatest threat—the trusted employee, who either unknowingly or maliciously causes problems on the network.

**What actions should organisations take to protect themselves from cyber crime?**

Rather than relying on a single product or a collection of products, organisations need to develop a comprehensive program with a fundamental objective of ensuring the confidentiality, integrity, and availability of data. Any such program encompasses a number of components, which include policy, disaster recovery, backup strategies, and the three critical security elements—physical security, application security, and the network or infrastructure security. A security program also includes a critical incident response capability, top-to-bottom training efforts, and provisions for assessing and testing system vulnerabilities or new technologies. There are other subcategories, but those are the critical components, with policy providing the foundation and the means of integrating the various elements.

Deploying the program has to be a widely shared responsibility. For example, the data does not belong to the IT department and especially not to the information security department—the data belongs to the organisational business units. They are critical players in identifying how the security program is going to support organisational goals and objectives. For example, business units must classify their data so appropriate resources can be dedicated to safeguarding it. It would not make sense to dedicate expensive security measures to data that has little or no value to the organisation.

**What is the role of the board and senior leadership as companies take action to protect themselves from cyber crime?**

The most important aspect of an information security program is the support of senior management. They have to say, somehow, that "we need to incorporate information security into our business objectives, and every individual is responsible for supporting that effort." Without

leadership's buy-in, no matter what you do, information security simply will not be a priority for the people who have to make it work—the users and the business units. If you get the unqualified support of management, the program will be successful. Anything short of that leads to an uphill battle.

**Has AARP been subject to a cyber attack—the recent "I Love You" virus, for example—and, if so, what did you learn from that experience?**

Fortunately, nothing that we have had to deal with has been devastating. We were extremely fortunate with the "I Love You" virus because we are on a different e-mail platform, so it didn't significantly affect us. But now we are migrating, so will the next one hit us? Conceivably. We're trying to take proactive steps to protect ourselves, and we are learning from others.

**What are the key steps a company should take if a cyber attack occurs?**

Preparation is everything. Effective information security efforts begin before an attack occurs. The critical factors for success are to have a comprehensive plan; make it a collective effort among IT, the business units, and IT security; and get buy-in from management. Identify the key roles and responsibilities, and be sure everyone knows their part. During a critical incident, the department can't operate in a vacuum—the responsible people have to work together, probably under the direction of an information security professional. That person can manage and co-ordinate the activities of others in support of the plan, thereby increasing the probability of quickly determining everything from the source of the attack to the extent of the damage and how to recover. If, on the other hand, the response is haphazard and without structure, the extent of the damage—much less where evidence may reside—may never be determined.

In addition, within an information security program, when and how to identify, collect, preserve, and even analyse evidence can be documented and prioritised. Traditionally after a critical incident, an IT staff's focus is on getting the business unit back in business. Frequently omitted are potentially important considerations, such as evidence collection, the potential for litigation, and when to notify law enforcement or internal forensic analysis. A comprehensive information security program can emphasise these considerations and get people talking about them long before a catastrophic event.

### Board Responsibilities in the Information Age—Recommendations from Olivia Kirtley

In a recent presentation to the Global Corporate Women Directors Colloquium: Emerging Trends in Corporate Governance, Olivia F. Kirtley, the immediate past chair of the American Institute of Certified Public Accountants (AICPA), offered a number of recommendations to directors about the questions they should be considering in an e-business environment, especially related to cyber crime.[21] Kirtley is a vice president at Vermont American Corp. as well as a director on the boards of ResCare, Inc., and Lancer Corp.

Kirtley noted that boards have the critical responsibility to assure that all assets of an organisation are protected, including its information. "The 'tone at the top' is just as critical for technology issues as it is for the quality of financial reporting," she said. "Directors have a fundamental duty to understand the changes technology has brought about as well as the implications of new risks, opportunities, and shareholder value. Although all technology-related exposures cannot be prevented, the board must assure that risks are identified, exposures minimised, and that information integrity, availability, and security are addressed within the overall business strategy."[22]

Kirtley recommends that directors consider the following questions—and be prepared to judge the adequacy of the answers, seeking outside and expert assistance, if necessary:

- Does the organisation have a chief IT officer? Why not?
- Does the organisation have a chief IT security officer? Why not?
- When was the last time the organisation's IT controls were reviewed? Was the evaluation performed internally or by an outside expert? What were the results? Have all recommendations been implemented or scheduled? If no recent review has been performed, when will it be and by whom?
- Does the organisation have a business continuity plan in the event its IT systems are disabled?
- Does it have a disaster recovery plan that is reviewed on a regular basis? By whom? Has it been tested? When?
- Is a systems audit performed periodically to assure that IT controls and security are sufficient to prevent unauthorised access to files, alterations of records, loss or theft of data and trade secrets, and misappropriation of information assets?
- Have the external or internal auditors reviewed the systems and controls? What were the results?
- Has the organisation been a victim of computer fraud by employees or others?
- Have hackers succeeded in breaking into the organisation's systems? How? What measures have been taken in anticipation of future attempts?
- Has a drill of hiring professional hackers to test the systems been done?
- Does the organisation outsource key technology functions? Does doing so create any potential reliability or continuity issues?

- What security or privacy mechanisms are in place with business partners, agents, and suppliers? Do those entities directly utilise systems and/or data?
- Has management updated its insurance coverage for new potential risks associated with on-line, e-business, and technology security exposures? Is the organisation's insurance consultant qualified to advise in this area?

Directors also need to ask questions on how technology is affecting the future of the organisation, because the answers can have a substantial effect on future shareholder value, notes Kirtley. Outside experts may be needed to evaluate the answers to these questions:

- How is the organisation keeping up with changes in IT?
- Is the organisation an industry leader in the use of IT?
- Are the organisation's management information systems state of the art?
- Will significant systems investments be needed to maintain the organisation's competitiveness?
- Does the organisation measure the investment in its IT systems to benchmark expenditures and performance against its peer group?
- What are the budgeted capital expenditures for IT this year? Over the next three years? How does this budget compare with other companies in the industry?
- What are the organisation's e-business plans and results to date?
- What are the major threats and opportunities to the organisation from e-business?
- Has the organisation lost market share to others that are using e-business more effectively?
- Does the organisation expect to downsize operations or to realise other savings as a consequence of dealing with customers directly on-line? How will the employment levels be effected?
- Is e-business receiving an appropriate level of senior management attention? Who is responsible for it? Has the organisation examined whether the right mix of management skills is in place to maximise the opportunities available?
- Is the organisation using the Internet to sell to customers directly rather than through traditional channels? Will this practice negatively affect traditional sales?
- Is the organisation using the Internet for procurement and managing its supply chain? What are the results in terms of new sources of supply, better prices and terms, and accelerating the procurement cycle?
- What is the organisation doing to protect the privacy of the personal data it gathers?

# Appendix III: Applying the Law to Cyber Invasions — An Interview with Meredith Fuchs

*As U.S. legislators debate the need for new laws to combat "new economy" crimes, a variety of avenues already exist in the United States for corporate victims to combat interference with legitimate online activities. Laws also are evolving internationally. Meredith Fuchs, an attorney with the Washington, D.C., law firm of Wiley, Rein & Fielding, addresses a number of these issues below.*[23]

**Can organisations fight back in cases of hacking or denial-of-service attacks?**

Various statutory remedies are available in the United States in both the criminal and civil context. The U.S. Computer Fraud and Abuse Act (CFAA) protects against attacks that cause damage to a computer, such as denial-of-service attacks. Civil compensatory damages and injunctive relief are available to any party who suffers economic damage or loss by reason of violation of the CFAA. "Damage" includes "any impairment to the integrity or availability of data, a program, or information that causes loss aggregating at least $5,000 in value during any one-year period to one or more individuals."

In addition, the U.S. Electronic Communications Privacy Act (ECPA) prohibits accessing without authorisation the facilities of an electronic communications service, or intentionally exceeding an authorisation to access such facilities, and thereby obtaining, altering, or preventing authorised access to wire or electronic communications. The ECPA also authorises a civil action for a violation of any of the rights under the ECPA by "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct is engaged in with a knowing or intentional state of mind." Damages are defined as the "sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but not less than $1,000." Thus, unlike the CFAA, which provides only for "economic damages," plaintiffs under the ECPA are entitled to the potentially more potent remedy of recouping a defendant's ill-obtained gains. Moreover, the ECPA permits recovery of attorneys' fees, and it also authorises the court to "assess punitive damages" in situations where the "violation is wilful or intentional."

Victims of denial-of-service attacks may also have common-law remedies. A "trespass to chattels"—which occurs when one party intentionally uses or meddles with personal property in rightful possession of another without authorisation—may take place when a hacker uses or meddles with a computer system. Similarly, the tort of "conversion" may apply to denial-of-service attacks. Conversion is the intentional exercise of dominion or control over personal property that so seriously interferes with the owner's right to control the property that the owner is entitled to receive the full value of the property. In cases in which a computer network or a Web site is unable to function as intended, the interference may be so significant as to substantially disturb the owner's possession of the network or site. The tort of "intentional interference with business relations" may also be applicable and offers a means to recover lost profits.

**Is it particularly difficult to come up with remedies in cases of hacking, where the U.S. (federal) law does not apply?**

Although the U.S. law does not specifically provide a civil remedy against hackers—without there being damage or without information being obtained without authorisation—some state courts have begun to recognise the possibility of a computer trespass cause of action that is

premised solely on unauthorised access to a computer. In many cases, however, some demonstrable damage will exist, and, thus, it is critical that businesses develop protocols for preserving evidence of intrusions. Organisations have a direct business interest in doing so, because the evidence may help stop the hackers as well as help the business improve its technological security measures.

In addition, several states are developing criminal anti-hacking statutes that will at the very least provide the possibility of criminal prosecution. The widespread anxiety about computer crimes and cyber terrorism, as evidenced by President Clinton's National Security Plan, will likely lead to additional legislation to combat these activities.

**How are the laws developing internationally? And how big a problem is the current lack of harmonisation among international laws?**

Countries worldwide do need to reach consensus as to which computer activities should be criminalised. The immediate and widespread proliferation of the "I Love You" virus demonstrates the reach of cyber activities. Yet the lack of criminal penalties in many countries leaves us without redress against wrongdoing initiated elsewhere.

Currently, the United States is a party to many international treaties that provide for some international support for prosecutions. In some situations, however, conduct must be considered criminal in both jurisdictions for the United States to obtain foreign assistance, and reaching that agreement can be difficult.

Moving forward, at the very least, we need increased monitoring and reporting of cyber security problems as well as coordination on issues related to the preservation of evidence. Several multilateral efforts are now underway to accomplish some of these goals. For example, the Council of Europe is drafting a Cybercrime Convention, to be completed in December 2000. Though not a member, the United States has participated in the project. In addition, the Group of Eight has a subgroup on high-tech crime that is considering computer criminal investigation and prosecution issues.

**So, overall, does a victimised business have realistic weapons it can use?**

Efforts are in place and under development to help organisations strike back. In circumstances where the perpetrator is a business seeking a commercial advantage, the prospect of obtaining a meaningful financial recovery is often quite realistic. Even where the attack comes from an individual without the resources to pay a substantial judgement, injunctions may be powerful weapons available to injured companies without relying on government law enforcement. Developing an effective legal response is a multi-layered effort, involving preservation of evidence, co-ordination with law enforcement, and a willingness to pursue remedies so as to deter future attacks.

# Appendix IV: Beyond the Internet — Exploiting Digital Telephony Services

The exploitation of network computer systems is a widely known phenomenon. However, digital telephony exploitation—where internal or external offenders gain unauthorised access to and misuse a business's computerised telecommunications switching system—is on the increase world-wide, although it remains relatively unknown or ignored in the shadow of Internet crime. Losses to businesses take two common forms: toll fraud (theft of billable calling services) and other asset losses through network exploitations.

Historically, digital telephony exploitation victimised telephone companies, causing them to focus on revenue losses stemming from toll fraud. In 1995, U.S. research estimated that the total cost of corporate telephony system toll fraud was $1.625 billion.[24] Professional toll fraud offenders in the form of "call-sell" operations have operated around the world for decades. These offenders traffic in stolen calling cards, devices to circumvent the tracking and registration of toll calls, or the theft and use of master passwords[25] to exploit digital telephony servers.

The threat of toll fraud now affects businesses other than telephone companies. Over the past decade, many businesses have created internal telecommunications networks using dedicated on-site digital telephony servers, also known as computerised branch exchanges (CBX), and incorporated voicemail technologies into their business infrastructures. CBXs are essentially computerised telephone switches. Unauthorised access into and manipulation of CBX capabilities by inside or external offenders could lead to "on-hook" audio interceptions, toll fraud, cyber network attacks, and crimes involving the use of voicemail systems. The exploitation of a corporate CBX, for example, could lead to the theft of calling services, the misuse of corporate voicemail technologies by criminal groups, the loss of proprietary information though electronic eavesdropping (corporate espionage), and the exposure of the business to civil litigation risk.

***Organisations must also be aware of the threats to their telecommunications networks and voicemail systems.***

CBX exploitation could stem from cyber misbehaviours and techniques similar to those found in Internet exploitations. CBXs frequently operate a variant of the UNIX operating system widely used on the Internet. Enterprises commonly interconnect their Internet networks with their CBXs to facilitate the cost-effective remote maintenance of both systems. Such actions expose both networks to exploitation by internal and external offenders.

Businesses can no longer afford to assess the security of their CBX systems separately from their Internet networks. As with the purchase and implementation of Internet technologies, however, many businesses do not fully understand the system administration challenges posed by CBXs and have not activated security features to minimise exploitations. Organisations must consider holistic assessments of all of their communications networks in the context of sound forensic incident response policies, procedures, and awareness training to mitigate risk and civil exposure.

[1] Illena Armstrong. "Computer Forensics: Investigators Focus on Foiling Cybercriminals," *SC Magazine*, April 2000.

[2] "The digital nervous system is Gates' term for how nations can employ technology to do a better job of managing and using information to create greater efficiencies in government operations; improve and broaden education; help businesses compete globally; and improve the way people live, learn and work." http://www.microsoft.com/BillGates/news/icontrip.htm

[3] Illena Armstrong. "Computer Forensics: Investigators Focus on Foiling Cybercriminals," *SC Magazine*, April 2000.

[4] *Investor's Business Daily*, May 17, 2000, Sec. A, p. 9.

[5] "Internet Users Now Exceed 100 Million," *The New York Times*, Nov. 12, 1999.

[6] Speech by U.S. Attorney General Janet Reno to the National Association of Attorneys General, Jan. 10, 2000. http://www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm

[7] Speech by U.S. Deputy Attorney General Eric H. Holder, Jr., at the High-Tech Crime Summit, Jan. 12, 2000. http://www.usdoj.gov/criminal/cybercrime/dag0112.htm

[8] In many cases, thousands of attacks are launched mindlessly. When launched by teenagers, the intruders are referred to as "script kiddies" since they are taking existing programs and directing the execution of those programs against specific targets.

[9] Illena Armstrong. "Computer Crime Spreads," *SC Magazine*, April 2000.

[10] Used in the broadest sense, "something of value" means data with meaning and value such as trade secrets, proprietary information, personal identification data, and so forth.

[11] http://www.internetnews.com/ec-news/article/0,2171,4_340591,00.html

[12] http://www.sjmercury.com/breaking/docs/062060.htm

[13] http://www.securityportal.com/cover/coverstory20000410.html

[14] http://www.currents.net/newstoday/00/04/18/news2.html

[15] Intruders learn about their victims by using Internet lookup or yellow page services, X.500 directories, or services running on hosts' machines; reviewing data in public directories; probing mail servers; and using non-network-based data about a victim.

[16] This practice is commonly called "social engineering."

[17] http://www.washingtonpost.com/wp-srv/WPlate/2000-03/02/2141-030200-idx.html

[18] Illena Armstrong. "Computer Forensics: Investigators Focus on Foiling Cybercriminals," *SC Magazine*, April 2000.

[19] Speech by U.S. Attorney General Janet Reno to the Virginia Journal of International Law, University of Virginia Law School, Charlottesville, Virginia, April 1, 2000. http://www.usdoj.gov/ag/speeches/2000/4100aguva.htm

[20] Telephone interview with Jeff Hormann conducted May 25, 2000.

[21] Kirtley developed her questions based on a variety of sources, including Big 5 materials on recommended questions for shareholders.

[22] Telephone interview with Olivia Kirtley conducted June 7, 2000.

[23] Telephone interview with Meredith Fuchs conducted June 6, 2000.

[24] Telecom & Network Security Review, Pasha Publications, U.S.A. 1995.

[25] Known as "Montebello's"

## KPMG's Forensic and Litigation Practice

The Forensic and Litigation practice provides a comprehensive range of investigation and litigation services to organisations in virtually every industry. KPMG assists organisations in uncovering, investigating, and preventing fraud and provides industry-focused litigation services throughout the dispute-resolution process, including financial and economic analysis, expert witness services, damage assessment, and industry-specific liability and transactional analysis.

## KPMG's Assurance and Advisory Services Center

KPMG's Assurance and Advisory Services Center (AASC) provides assistance to KPMG member firms in creating, enhancing, and supporting KPMG member firms' assurance products worldwide. Staffed by client service and technical professionals recruited from KPMG member firms around the world, the AASC is a center for assurance research and innovation, product development and support, knowledge management, and technology tool integration.

## Major KPMG Contributors

Tom Talleur
Kurt Beyer
Paul Bull
Susan Rucker
Diane Kiffin Nardin
KPMG's Department of Professional Practice
KPMG's Assurance Marketing Department

**Visit us on the World Wide Web at www.kpmg.com.**



20813atl