Deloitte.

Cyber crime: a clear and present danger

Combating the fastest growing cyber security threat

Center for Security & Privacy Solutions

Contents

Introduction

Threats posed to organizations by cyber crimes have increased faster than potential victims—or cyber security professionals—can cope with them, placing targeted organizations at significant risk. This is the key finding of Deloitte 's review of the results of the 2010 CSO CyberSecurity Watch Survey, sponsored by Deloitte and conducted in collaboration with *CSO Magazine*, the U.S. Secret Service, and the CERT Coordination Center at Carnegie Mellon (see sidebar on page 4).

This whitepaper reports several key results of this survey and Deloitte's interpretation of key survey results. By its nature, interpretation goes beyond simple reporting of results (which is not our goal here) and may prompt disagreement or even controversy. Deloitte believes however, that some of the findings point to significant incongruities between the views of many survey respondents and the current reality of cyber crime. Given that the survey respondents include mainly executives and professionals responsible for the security of their organizations' IT environments, such incongruities are worth examining.

Our view is that the growth of the threat of cyber crime has outpaced that of other cyber security threats. From our perspective, the 2010 CSO CyberSecurity Watch Survey, viewed in the light of our experience, indicates that cyber crime constitutes a significantly more common and larger threat than respondents recognize. Indeed, driven by the prospect of significant profits, cyber crime innovation and techniques have outpaced traditional security models and many current signature-based detection technologies.

Today's cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments. Meanwhile, many organizations may be leaving themselves vulnerable to cyber crime based on a false sense of security, perhaps even complacency, driven by non-agile security tools and processes. Many are failing to recognize cyber crimes in their IT environments and misallocating limited resources to lesser threats. For example, many organizations focus heavily on foiling hackers and blocking pornography while potential—and actual—cyber crimes may be going undetected and unaddressed. This has generated significant risk exposure, including exposure to financial losses, regulatory issues, data breach liabilities, damage to brand, and loss of client and public confidence.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP.
Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Stealth techniques enable cyber criminals to act without fear of timely detection, let alone capture and successful prosecution. It is among some of the most insidious—and profitable—of crimes, and can be conducted from a well-equipped workstation, perhaps within your own organization.

Major threats and risks to data, information, assets, and transactions are continually evolving, and typical approaches to cyber security are not nearly keeping pace. Current security models are minimally effective against cyber criminals *and* organizations remain unaware of that fact.

Cyber criminals seem to be reinvesting portions of their significant profits in developing new capabilities for circumventing today's security technologies. Indeed, even major antivirus vendors find it difficult to keep up with the amount of new malware "in the wild." Cyber criminals routinely exploit the resulting vulnerabilities. Moreover, they can now target the weakest link in most security models—the end user—through the Internet by means of social engineering techniques. (The latter refer to scams and ruses criminals use to make a user believe they are co-workers, customers, or other legitimate parties.) Stealth techniques enable cyber criminals to act without fear of timely detection, let alone capture and successful prosecution. It is among some of the most insidious—and profitable—of crimes, and can be conducted from a well-equipped workstation, perhaps within your own organization.

This whitepaper shows how Deloitte's view of the threat of cyber crime differs from the perceptions indicated by responses to the 2010 CSO CyberSecurity Watch Survey. It discusses the ways in which cyber security threats and risks have changed in recent years, how to more accurately assess them, and how to more effectively combat them.

More broadly, this paper is designed to:

- sound an alarm regarding new cyber security priorities
- describe the form and magnitude of the threats posed by cyber crime
- suggest useful responses to mitigate these threats

This paper is directed toward senior leaders including CIOs, CSOs, CROs, operational risk managers, government agency budgeting and procurement professionals, and other executives and professionals with decision-making roles in the security of their organization's IT environment and of the assets within that environment.

About the 2010 CSO CyberSecurity Watch Survey

The 2010 CSO CyberSecurity Watch Survey was sponsored by Deloitte and conducted in 2009 in collaboration with *CSO Magazine*, the U.S. Secret Service, and the CERT Coordination Center at Carnegie Mellon. Survey respondents contributed a broad and valuable set of perspectives.

The 523 respondents primarily included directors or managers of IT or security (33 percent), and C-suite executives, such as CEOs, CFOs, CIOs, and CSOs and executive vice presidents (32 percent). Also included were law enforcement professionals (11 percent), various staffers (13 percent), and consultants (8 percent).

Respondents came from the private sector (69 percent) and public sector (31 percent). Among the private-sector respondents, 86 percent were from for-profit enterprises and 14 percent were from non-profits. Among the public-sector respondents, 29 percent were from the federal government and 79 percent from state and local government.

Cyber crime update

An increasing number of criminals and criminally minded enterprises have hired, purchased, or otherwise acquired the ability to infiltrate systems with new penetration techniques while developing a criminal e-business network. Concurrently, an increasing number of hackers have turned professional. Some who once attacked IT systems for the intellectual challenge and to match wits with (or to aggravate) others in their field have discovered strong financial rewards in online crime.

Trends that demand a bold response

In addition, the following key cyber crime trends have emerged, and they demand a strong, bold, near-term response:

- Cyber attacks and security breaches are increasing in frequency and sophistication, with discovery usually occurring only after the fact, if at all.
- Cyber criminals are targeting organizations and individuals with malware and anonymization techniques that can evade current security controls.
- Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense and are rapidly becoming obsolete—for instance, cyber criminals now use encryption technology to avoid detection.
- Cyber criminals are leveraging innovation at a pace which many target organizations and security vendors cannot possibly match.
- Effective deterrents to cyber crime are not known, available, or accessible to many practitioners, many of whom underestimate the scope and severity of the problem.
- There is a likely nexus between cyber crime and a variety of other threats including terrorism, industrial espionage, and foreign intelligence services.

Today's stunning cyber-crime trends demand a strong, bold, near-term response.

Future indicators

Here is real cause for alarm: most indicators point to future cyber crime attacks being more severe, more complex, and more difficult to prevent, detect, and address than current ones, which are bad enough. An underground economy has evolved around stealing, packaging, and reselling information. Malware authors and other cyber criminals for hire provide skills, capabilities, products, and "outsourced" services to cyber criminals. These include data acquisition and storage, stealthy access to systems, identity collection and theft, misdirection of communications, keystroke identification, identity authentication, and botnets, among others. Meanwhile, today's security model is primarily "reactive," and cyber criminals are exploiting that weakness.

As a result of such developments, data breaches have occurred in many organizations which appear to have deployed traditional security controls, processes, and leading practice architectures, including the following representative instances in 2008 and 2009:

- At a major online service provider, more than one-half million credit card accounts were put at risk by malware, to be discovered four months later.
- At a major online payment facilitator, over one hundred million credit card accounts were put at risk by malware over an unknown period before discovery.
- Malware on an online booking system exposed some eight million personal records to risk.
- Malicious software on cash register terminals at a regional restaurant chain compromised thousands of credit and debit card accounts and, separately at a major supermarket chain, over four million credit card accounts.
- Website intrusion compromised tens of thousands of customer records at an auto repair chain.

Cyber criminals now operate undetected within the very "walls" erected to keep hackers out. Their technologies include rogue devices plugged into corporate networks, polymorphic malware, and keyloggers that capture credentials and give criminals privileged access while evading detection. These technologies are a reason why so many breaches are detected only after significant exposure has occurred. An unknown number of such cases are likely never detected, particularly when a cyber criminal skims a few cents off millions or tens of millions of transactions or exfiltrates data hiding in the noise of legitimate outbound traffic.

Several additional developments have heightened the current cyber crime wave:

- Social networking and constant online communication—and the proliferation of communication devices, networks, and users—have generated new vulnerabilities that create more cyber crime opportunities.
- Online banking, investing, retail and wholesale trade, and intellectual property distribution present countless opportunities for theft, fraud, misdirection, misappropriation, and other cyber crimes.
- Foreign rogue governments, terrorist organizations, and related actors sometimes exploit cyber vulnerabilities to help fund their espionage, warfare, and terror campaigns.
- Organized crime has extended its reach into cyberspace, adding cyber crime to its portfolio of "businesses."
- Economic hardships spawned by the 2008-09 recession may generate resentment and financial motivations that can drive internal parties or former employees to crime. In fact, "wire mule" may be a new job opportunity in the emerging "new economy."

This is a picture developed over the past several years of working with a diverse portfolio of clients on a broad range of risk management and security challenges. We drew upon that experience in reviewing the responses to the 2010 CSO CyberSecurity Watch Survey, and developed an interpretation that led to what may be viewed as counterintuitive or even contradictory conclusions about the current state of cyber crime and organizations.

Deloitte's view of the cyber crime scene

Awareness or complacency

Deloitte believes the survey responses reveal a serious lack of awareness and a degree of complacency on the part of IT organizations, and perhaps security officers, vis-à-vis the threat of cyber crime. Much of this belief is predicated on the notion that cyber crime technologies and techniques are so effective at eluding detection that the actual extent of the problem may be grossly underestimated. Although we cannot quantify the financial impact of cyber criminal activity, we would like to highlight a comment made last year to help establish some potential statistics. Last year, the White House issued the Cyber Security Policy Review, which profiled the systemic loss of U.S. economic value from intellectual property and data theft in 2008 as high as $1 trillion.[1]

In this section, we will first summarize our view and then examine areas of divergence with selected survey responses. Some of our views will not surprise security and IT professionals in industries characterized by high vulnerability or organizations that have experienced some degree of cyber crime. Other readers may find our view of the seriousness of cyber crime surprising. Our purpose here is to provide an updated, broad, but well-supported view of the cyber crime threats that we perceive as most serious *and* to present potentially more effective ways of addressing these threats.

Essentially our view is that:

1. Cyber crime is now serious, widespread, aggressive, growing, and increasingly sophisticated, and poses major implications for national and economic security.
2. Many industries and institutions and public- and private-sector organizations (particularly those within the critical infrastructure) are at significant risk.
3. Relatively few organizations have recognized organized cyber criminal networks, rather than hackers, as their greatest potential cyber security threat; even fewer are prepared to address this threat.
4. Organizations tend to employ security-based, "wall-and-fortress" approaches to address the threat of cyber crime, but this is not enough to mitigate the risk.
5. Risk-based approaches—and approaches that focus on what is leaving the IT environment as well as on what is entering it—hold potentially greater value than traditional security-based, "wall-and-fortress" approaches.
6. Organizations should understand how they are viewed by cyber criminals in terms of attack vectors, systems of interest, and process vulnerabilities, so they can better protect themselves from attack.

Given this view, Deloitte suggests most organizations should consider a continued risk-based approach to cyber security along with a renewed focus on deeper analysis of their inbound and outbound network traffic. Such an approach incorporates the potential vulnerability to and impact of cyber crime, along with other, perhaps more familiar and measurable risks, such as unauthorized trades and foreign currency risk. We suggest specific methods for detecting and addressing cyber criminal activity later in this paper.

[1] White House Cyber Policy Review: "Assuring a Trusted and Resilient Information and Communications Infrastructure", May 29, 2009, http://www.whitehouse.gov/cyberreview/

Deloitte's interpretation of survey findings

A number of the responses in the 2010 CSO CyberSecurity Watch Survey tend to contradict the experience of Deloitte in the field, and point to potential misunderstanding of cyber threats and risks and of optimal approaches to cyber security.

Specifically, we interpret the following results in the following ways:

Situational Awareness: Hackers were rated the greatest cyber threat, over insiders, criminal organizations, and foreign entities. Given that 69 percent of respondents were private sector, that's understandable. However, organized crime and foreign entities were rated lower than Deloitte's assessment would indicate as warranted. This may point to a misunderstanding of the external operating and threat environments. Organizations may focus on unsophisticated attacks from hackers because they are the noisiest and easiest to detect. Yet that focus can overlook stealthier attacks that can produce more serious systemic and monetary impacts. Attackers from nation states and organized crime syndicates deploy more sophisticated techniques which may go undiscovered.

Implication: Organizations can develop situational awareness in various ways, and thus detect and recognize threats and damages that now go undetected and unrecognized. Attention to behavioral indicators tied to fraudulent activities is a must.

Preparedness: The vast majority of respondents—over 75 percent—reported that monetary losses from cyber security events either remained the same (in comparison to the previous year) or they weren't sure. In addition, over 70 percent of respondents reported that their organization was not specifically targeted by cyber criminals or other actors but just happened to be impacted by "non-specific or incidental attacks." In our view, respondents appear to underestimate the threats and to have relatively little situational awareness, yet 58 percent also rate themselves as more prepared to deal with threats. This may reflect lack of knowledge regarding the type of infiltration and damage that is occurring within the environment. Typically, there is an inverse correlation between situational awareness and perception of preparedness, and cyber criminals are counting on this disconnect.

Implication: Organizations that are unprepared or under-prepared often fail to recognize that fact. A shift in perspective away from a wall-and-fortress, authorization-driven approach toward one focused more on what is leaving the internal environment—and on what happens to it after it leaves—can help remedy this situation.

Spending does not equal security: A large number of respondents (47%) indicated a significant level of spending on IT security last year ($100,000 or more). Higher spending does not necessarily yield greater security. We see many organizations allocate significant resources to technological security measures, but neglect simple, inexpensive measures such as patch management, log analysis, privilege restrictions, password expiration, and termination of former employees' access through a robust deprovisioning process.

Implication: Many organizations can implement easy, inexpensive, but often overlooked fixes that increase security. Often these measures can help mitigate threats with potentially serious consequences. However, even these measures alone may not be sufficient to significantly improve security against the evolving cybercrime threat. Methods such as the risk-based approaches suggested below would likely be necessary in most organizations.

Organizations would also do well to understand the security priorities and systems of their key vendors, business partners, and suppliers, and to share such information about their organizations with these parties. Cyber security is ordinarily enhanced by a multilateral, team approach.

In fact, some organizations may be misinterpreting the nature of the breaches they experience. The 2010 CSO CyberSecurity Watch Survey found that of the organizations that experienced cyber security events that caused financial loss or cost during the preceding 12 months, only 28 percent found the events to be specifically aimed at them. That's up from 22 percent in the previous (2007) survey, but it still strikes us as low. It seems to us that a substantially larger percentage of the incidents may have actually targeted the organizations, particularly since they involved financial loss or costs. These statistics may reflect the insidious nature of cyber crime attacks, in that victims often don't know they were the intended victims.

In the 2009 survey, only 6 percent of respondents cite "organized crime" as the greatest security threat to their organizations. That slightly outranks the percentage who see the greatest threat as emanating from foreign entities (5 percent), current service providers and contractors (4 percent), customers (3 percent), and competitors (3 percent).

Yet it ranks far below the percentage who see the greatest threat emanating from hackers (26 percent) and current employees (19 percent).

The definition of "hacker" and for that matter "organized crime" may vary from respondent to respondent. Hackers can morph into criminals, organized and otherwise. Also, organized crime is not limited to many people's definition of the term, which often includes only the drug smuggling cartels and other operations covered regularly in the media. And what about the myriad of skilled initials and hacker groups who may establish informal alliances with terrorist organizations, foreign intelligence services, and even traditional organized crime entities specifically for the purpose of selling their services? The problem may be even worse than imagined.

The focus obscures the view

Users as mules

Most cyber security focuses on preventing attacks and unauthorized usage. It is this very focus that can allow and even enable cyber criminals to employ legitimate users as unwitting accomplices. Authorized users can access and travel throughout a system, remove or change data in the system, and conduct transactions. When cyber criminals employ such users as unwitting accomplices or "money mules," they can operate as if they were users. They can acquire the same, or even greater, ability to navigate pathways, copy data, execute transactions, and monitor keystrokes.

It is that kind of activity that must be detected, prevented, and addressed. Of course, practices designed to secure the environment and data and to detect traditional breaches must remain in place. But sophisticated cyber criminals have studied the methods organizations use to both "wall off" and grant access to their networks and data. This positions criminals to conduct activities that can go undetected for months, or to commit a single, major, extremely profitable and damaging crime, such as wire transfer fraud. In many cases cyber criminals have obtained credentials and accessed systems as if they were actual employees and customers. Thus, the integrity of the endpoint that is being granted access to the organization's systems and data must be a primary concern.

The public sector is as exposed as the private sector. There have been cases in which state-level government agencies in the United States have lost measurable monetary sums. For example, the July 2, 2009 entry on *Washington Post* reporter Brian Krebs' blog stated that Ukrainian cyber criminals had stolen $415,000 from a county by means of unauthorized wire transfers from the county's bank. The criminals were aided by more than two dozen co-conspirators in the United States.

Krebs reported that his source, an investigator on the case, noted that the criminals used "a custom variant of a keystroke logging Trojan" that promptly sent stolen credentials to the attackers by instant messenger. This malware also enabled the attackers to log into the victim's bank account by using the victim's own Internet connection. Similarly, $480,000 was stolen from a bank account of a county Redevelopment Authority by means of Trojan malware. Threats from cyber crime at federal agencies could extend to matters of national security.

Shifting the basic approach

One of the more fruitful approaches to consider in addressing the threat of cyber crime involves moving from a primarily security-based approach to a more risk-based approach. Blocking what is coming into the environment—the strength of the security-based approach—is useful and necessary. However, that can often be accomplished less expensively and perhaps more selectively.

Shifting the focus to include monitoring and identifying data that *leaves* the environment can detect activities enabled by techniques and technologies that mimic, exploit, or piggyback on the access of authorized users. Relevant items may include user credentials, personally identifiable information, financial data, and vulnerability details. Current security wall, access control, and identity authentication approaches typically won't identify criminal activity geared to capturing that data and information.

With their current methods, cyber criminals can even infiltrate systems of organizations that hire "white hat" hackers to test their defenses. Cyber criminals view a system from a process perspective with the goal of gaining access as an actual user would. They then focus on acquiring the access and authentication tools that an actual user would have. Once inside a system, cyber criminals can use it in ways that the organization did not, and cannot, anticipate or defend against. While security personnel are intently watching their Security Information Manager screens, the cyber criminals are already inside.

A risk-based approach to cyber security

A risk-based approach can start with the assumption that an unauthorized user *can gain access* to the system, and then design responses based on the value of the data that could thus be compromised. This calls for prioritizing data and information based on value to the organization or other useful criteria. The organization can then decide which data to focus which resources on, how much to spend, and which tools to use to protect data.

This approach can help the enterprise shift away from building a "great wall" against all threats, toward identifying and addressing the most significant ones. This entails prioritizing risks on the basis of their likelihood, impact, and potential interactions with other risks, then allocating resources accordingly. It takes effort, expense, training, and resources to develop a system of categorization by value and to track data after it leaves the organization, but it pays off in efficiency and effectiveness. It is also possible to risk-rank data by type, value, and impact if it were to be compromised.

Relatively few organizations have developed categories based on value or risk. However, identifying which data is most and least valuable enables cyber security professionals to focus on the highest priorities. The most valuable data, such as product formulations and sensitive financial and legal information, can be tagged and monitored so that the organization knows where it is, where it is going, where it has gone, and on whose authority. Resources can then be shifted away from less valuable data, such as Website activity and routine email content, which can be treated accordingly.

…entails prioritizing risks on the basis of their likelihood, impact, and potential interactions with other risks, then allocating resources accordingly. It takes effort, expense, training, and resources to develop a system of categorization by value and to track data after it leaves the organization…

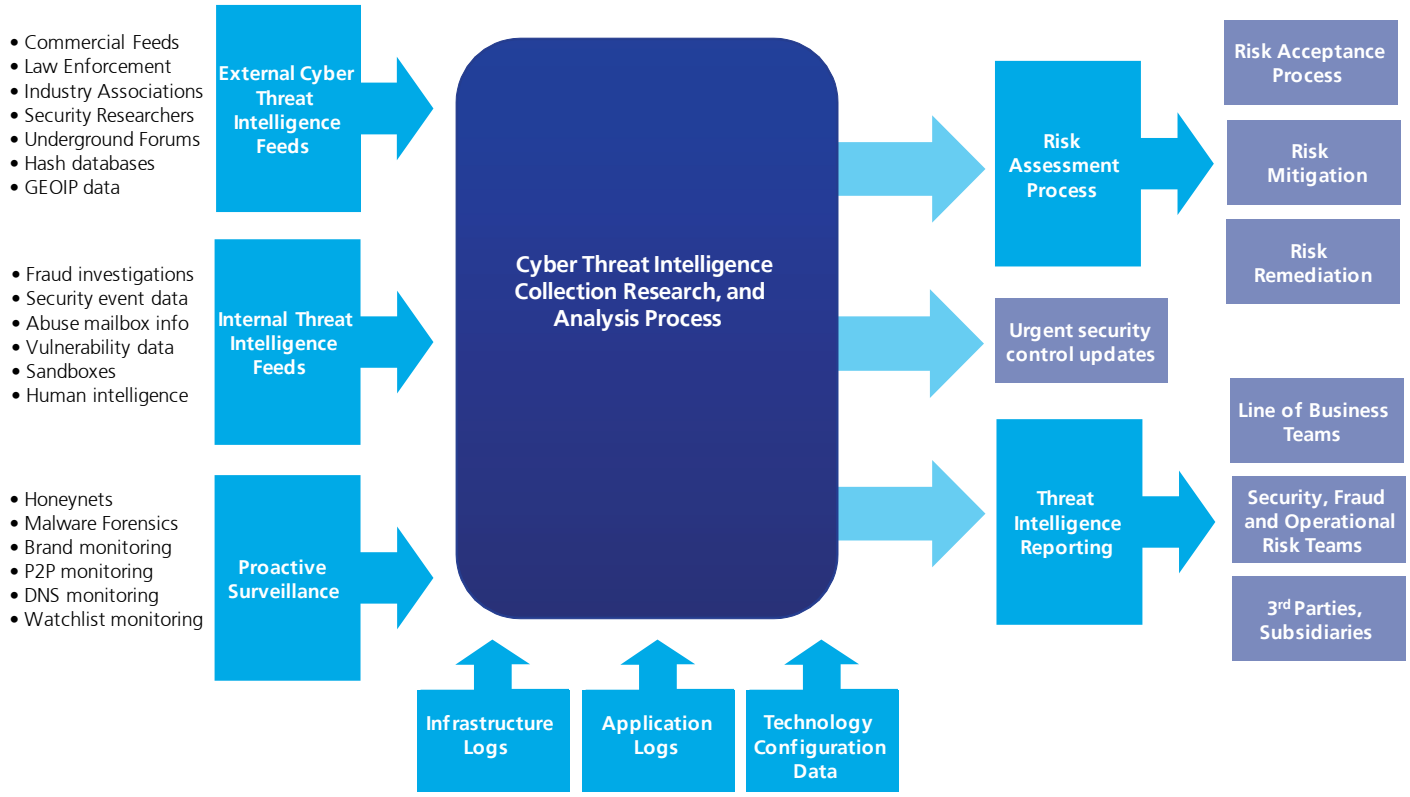
Developing "actionable" cyber threat intelligence

Combating cyber crime requires commitment from senior executives and board members. Yes, their plates are full. However, addressing cyber crime falls within risk management, an item already on their plate. Cyber crime is best addressed in the context of the organization's overall risk management approach. That way, it becomes an item in the IT, security, and risk management budgets and on the agenda at management and board meetings.

Once the commitment is made, several specific steps can improve cyber security and, incidentally, protection against other threats. These steps within Deloitte's approach focus first on intelligence gathering and analysis, then on assessment. The overall process is summarized in Exhibit 1. In practice, this process is best applied to specific areas—activities, data sets, delivery channels, and aspects of the IT infrastructure.

Identifying these areas takes time and resources, but they can be identified in the context of an overall risk management system. If a detailed enterprise-wide risk assessment has already been conducted, so much the better. That assessment will have identified critical processes, activities, data, delivery channels, and other resources, which can be employed in this effort.

Exhibit 1. Cyber intelligence acquisition and analysis



Intelligence gathering

Gathering intelligence is a continuous activity. For our purposes here, it involves choosing "promontories" from which to scan the external environment and monitor the internal environment. Another way to think of them would be as "channels" (akin to radio or television channels) through which you can monitor these environments.

Promontories or channels include those that constitute external cyber threat intelligence feeds and internal cyber threat intelligence feeds, as listed in Exhibit 2.

Exhibit 2. Cyber threat intelligence sources

External intelligence feeds	Internal intelligence feeds
• Publications	• Fraud investigations
• Law enforcement sources	• Security event data
• Industry associations & ISACs	• Abuse mailbox information
• Security vendors	• Vulnerability data
• Underground forums	• Sandboxes
• Hash databases	• Human intelligence
• GEOIP data	

While it pays to cast a wide net, there is always the factor of cost and the danger of sacrificing depth for breadth. So pick and choose your "feeds" given your industry, needs, and capabilities. Not every source will be useful to every organization, and some will be more useful than others to a given enterprise.

Proactive surveillance rounds out the intelligence gathering effort. Resources here include honeynets, malware forensics, brand monitoring, P2P (peer to peer) monitoring, DNS monitoring, and watchlist monitoring.

A few of the specific technologies on which to focus threat research include the following:

- ***Internet applications:*** online transactions, HR systems, wire systems, Websites
- ***Mobile computing:*** Blackberries, Smart phones, cellular networks, text messaging services
- ***Personal computers:*** operating systems, third-party applications, USB storage devices
- ***Banking devices:*** ATMs, kiosks, RFID enabled smartcards
- ***Intranets:*** intranet portals, collaboration tools, authentication systems
- ***Telephony:*** voice response units, VoIP phones and PBXs, voicemail
- ***Identity management and authentication:*** log-on, password, user code, and other IdM technologies

Another potential source of intelligence would be the resources that potential adversaries use. Again, the goal should be to focus on devices and applications that expose the organization's most valuable data, processes, activities, and infrastructure to the most risk. Once a rich mix of intelligence is being acquired, efforts turn to analysis.

Intelligence analysis

The amount of data derived from broad-based intelligence gathering can be staggering. Therefore, analysis includes statistical techniques for parsing, normalizing, and correlating findings, as well as human review.

Six questions should drive this analysis:

- How can we improve our visibility into the environment?
- What new technologies do we need to watch for and monitor?
- Do we have vulnerable technologies and data?
- To what extent will our existing controls protect us?
- Which industries are cyber criminals targeting and which techniques are they using and planning to use?
- How can we identify actionable information?

This analysis should be conducted within a risk management process built around well-defined risk identification, prevention, detection, communication, and mitigation activities. We won't delineate that process here, because most readers will be familiar with it. A cyber risk management process prioritizes threats, analyzes threats, detects a threat before, during, or after actual occurrence, and specifies the proper response. The latter may consist of remediation, control updates, vendor or partner notification, or other actions. Analysis, such as failure modes and effects analysis, provides a feedback mechanism, such as lessons learned, to constantly improve the effectiveness of the analytics being performed.

Benefits of a risk-based approach

In light of the potential risks of cyber crime, Deloitte recommends a risk-based approach, as outlined above. This contrasts with—but also augments—security-based approaches geared to walling off the IT environment. The benefits of a risk-based approach include the ability to:

- Define the value and risk-related significance of categories of data and to prioritize and protect them accordingly.
- Identify and mitigate devices inside the organization's network that are being used to support cyber criminal activities.
- Identify customers, suppliers, service providers, and other parties that have compromised devices inside their networks.
- Monitor transactions to identify those being conducted from compromised devices.
- Track compromised data that has left or is leaving the organization.
- Understand the organization's susceptibility to persistent, sustained access by cyber criminals.

Given the sophistication, complexity, and evolution of cyber crime technologies and techniques, no sizable organization can plan and implement the necessary response alone. CIOs, CSOs, CROs, and cyber security professionals should share information, techniques, and technologies in their battle against cyber crime. This can be done without revealing sensitive corporate or competitive information, but it had best be done.

In general, effective cyber security efforts require perspectives and expertise beyond those that reside in the organization. Thus, a 2010 CSO CyberSecurity Watch Survey finding that we found disappointing—and surprising—was that only 21 percent of respondents reported participation in their industry-sector IT-Information Sharing and Analysis Center (IT-ISAC). These communities of security specialists are supported by federal leadership, but much work remains if they are to become true public-private sector collaborations as originally intended. They certainly require the support of the cyber security community if they are to succeed.

Summing up the cyber crime dilemma

Data is more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money. The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities. The world has not changed much since the early 1900's when Willie Sutton was asked why he robbed banks. He said, "That's where the money is." Today, cyber criminals go where the data is because it gives them repeated access to the money, wherever it is.

Data is more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money. The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities.

Cyber crimes may pose the most potentially damaging threat to IT-related activities, transactions, and assets. We see this threat as under-recognized and under-rated among the risks that organizations face, and thus believe that many organizations are unprepared to detect, address, or protect themselves from these threats.

A vigorous, rapidly growing underground economy supports cyber crime activities. That economy includes organized crime, hackers for hire, disgruntled current and former employees, and other insiders (meaning people who have or had authorized access), and terrorists and their supporters. Cyber crimes include thievery, fraud, misdirection of communication, identity theft, intellectual property theft, corporate espionage, system sabotage, data destruction, money laundering, and terrorism, among others.

Some organizations' lack of preparedness stems from their traditional "wall-and-fortress" approaches to cyber threats. These approaches rest on access control and authorization technologies and techniques. However, cyber criminals can now not only circumvent many of these approaches but use them to gain the access that authorized users enjoy. Cyber criminals also have technologies that enable them to take advantage of that access in a matter of seconds.

Organizations can take several steps to protect themselves. The first step is to comprehend the seriousness of cyber crime threats to valuable data, processes, and assets. The second is to shift from a security-based approach to more of a risk-based approach to cyber security. Spend your budget and apply your resources to mitigate the highest ranking risks to your enterprise. The third step is to knock down the walls associated with siloed approaches of dealing with cyber threats. Sharing and combining data across the organization, for instance on fraud, loss prevention, information security, and human resources, while combining it with external sources strengthens the ability to perform value-added analysis.

At that point the organization can prioritize the risks, incorporate them into business decision-making processes, and manage them accordingly, with resources allocated more efficiently and effectively. Efforts then turn to information gathering and analysis, with an eye toward identifying cyber crime methods and threats and to monitoring assets as they are accessed and as they leave and after they leave the IT environment.

We do not suggest that cyber security professionals consider a change in focus and additional duties lightly. However, we do suggest that organizations consider their exposures to cyber crime and their current detection, prevention, and mitigation capabilities. Given the profits and current conditions, cyber crime may well be coming to your neighborhood—if it has not already moved in. More importantly, how would you know?

For more inofrmation

For current information on Center research, thought leadership, security events, or videos, please visit us online at www.deloitte.com/securitysolutions. Find our Center content on YouTube, or to subscribe to updates on our programs and solutions, register here www.deloitte.com/us/securityandprivacysolutions.

Ted DeZabala
National Managing Principal
Center for Security & Privacy Solutions
Deloitte & Touche LLP
+1 212 436 2957
tdezabala@deloitte.com

Rich Baich
Principal
Deloitte & Touche LLP
+1 704 887 1563
jbaich@deloitte.com