Are you compromised but don't know it?

A new philosophy for cyber security

January 2011

pwc

Table of contents

Heart of the matter

Assume a state of compromise

A new cyber security philosophy

Time and again, we find the same common denominator across cybercrime investigations: Digital evidence and breach indicators were present in the environment long before the victim became aware of the breach. Had those breach indicators been recognized, the victim could have intervened and minimized risk.

Transnational criminal enterprises often maintain remote access to the target environment for six to 18 months before they are detected. Our experience suggests that many state-sponsored cyber intrusions result in lingering unfettered access for many years, which in some cases is never detected. When it is discovered, recognition of advanced cyber intrusions does not typically come via in-house technology, processes, or people, but, rather, through third-party tipsters such as domestic law enforcement, intelligence sources, customers, or business partners.

When foreign governments, organized crime, or hackers target an organization, the techniques they use to compromise the network and enable sensitive data theft are well planned and methodical. Advanced cyber threat groups are extremely patient, tending to invest heavily in the research and development of custom malicious code and clever means to exfiltrate data; all designed to slip past the cyber security radar.

Today's advanced cyber threats are 2-pronged: to steal targeted data or disrupt services and to maintain access to the environment for as long as possible, thus enabling future intrusions. These threats apply to all industries, not just those that deal with payment cards or personal information. Companies that have proprietary data that is perceived to be of economic intelligence value, or any US company contemplating or already involved with international business transactions, are likely targets as well as their external law firms.

The future of cyber security is going to require an evolved philosophy that assumes a state of compromise.

Read on to learn more about how you can better protect your business from cyber threats by applying a new philosophy to cyber security which is founded on the realities of the cyber threat landscape.

An in-depth discussion

A never-ending cycle of incident response

Recognizing breach indicators

Basic breach indicators of an active but undetected cyber intrusion can include:

- Unauthorized web pages created on an Internet-facing web server
- Data transmitting outbound over unlikely protocols
- Large compressed files being transmitted outbound
- Unusual connections between a user systems using native operating system networking features
- Log entries on domain controllers capturing the execution of unauthorized programs

In most cases, this intelligence was available for days, months, or years at the many organizations which have engaged us to investigate cyber intrusions after they have occurred. Can your organization detect these breach indicators? Are there breach indicators everywhere but missed? Has your environment been compromised or is it currently being compromised? Is data and/or email being pushed out of your environment, literally right now?

You can get these answers by leveraging elements of reactive cybercrime investigations to help improve cyber security and reduce a myriad of related organizational risks. When our clients engage us to apply a cybercrime investigators mindset to assess their IT environment for an active but undetected intrusion, we have found that on average 3-5% of the client's computers are compromised.

We recommend adopting a new and evolved cyber security philosophy that accepts one reality: An ongoing state of compromise and incident response will be never-ending. A state of compromise will be unique for any given business, its industry, its areas of operation, its business partners and vendors, and how the cyber threat landscape relates to these factors.

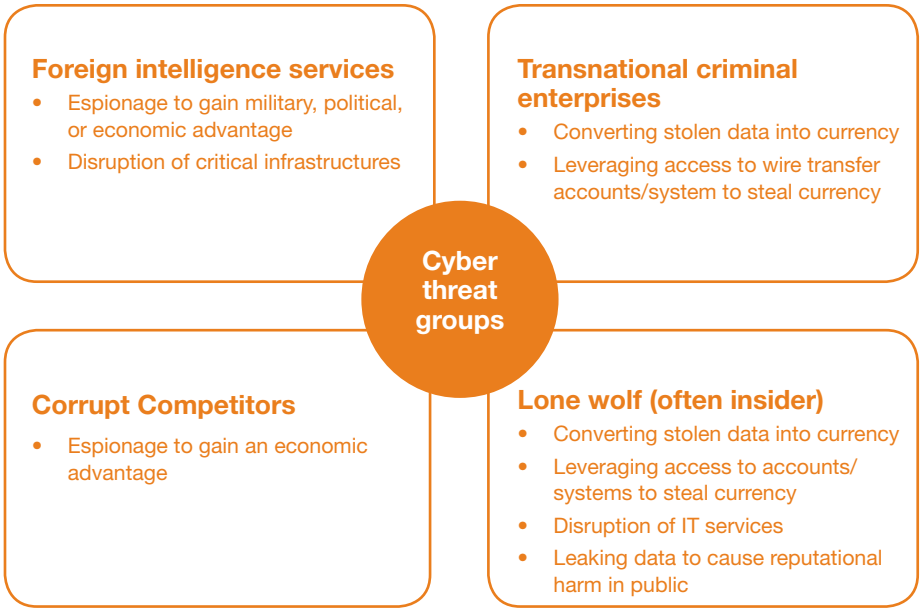
The cyber threat landscape

Cyber threats are varied, complex, and continuously evolving. History shows that preventive and defensive measures can reduce risks related to acceptable use violations, computer or network intrusions, data loss/leakage, and asset sabotage. However, the cyber threat landscape which involves targeting specific companies or industries is keenly aware of these cyber security strategies.

Cybercrime is committed by a multitude of offenders with diverse motives:

- Insiders who have authorized access and behave badly
- Competitors seeking advantage
- Foreign governments commit espionage for political or economic gain
- Transnational criminal enterprises steal and extort to generate income

The intelligence services of foreign governments are the most sophisticated, organized, and funded. Foreign Intelligence Services steal commercial Intellectual Property (IP) and business transaction information to gain an economic advantage and abscond with classified government information to gain a military or political advantage. Also, maintaining remote access for as long as possible is a primary objective of state-sponsored groups in order to execute future operational orders.



In one such case, PwC was engaged after a client was notified of a cybercrime by a US law enforcement agency that had been investigating a national security matter. After law enforcement advised the client—a critical infrastructure organization—that its private cyber space had been compromised, our forensic investigation uncovered the methods and techniques the state-sponsored actor had used to steal economic intelligence; we also identified the mechanisms that were enabling persistent remote access. We identified breach indicators and digital evidence that had been in the IT environment for years. Although the focus of this cyber intrusion appeared to be the gathering of economic intelligence, we worked with the victim to determine if the infiltration additionally compromised systems that could be used to disrupt critical infrastructure operations and create a national security nightmare.

The phrase 'transnational criminal enterprises' was crafted in recent years to replace the traditional tag, 'organized crime.' While a decade ago, organized crime groups hired hackers to compromise computers and steal data, today hackers, have formed their own global groups and underground networks and work independently of the traditional organized crime groups. The primary motive of these global criminal enterprises: sheer profit.

PwC has been engaged by clients who suspect that their environment has been compromised and that payment card or personal identity data has been stolen. In one of our recent investigations, some of the criminals' persistence and data exfiltration techniques closely resembled state-sponsored intrusions. We found multiple remote access methods that used custom malware, which at the time, were not known to the public and law enforcement. Had we wrapped the investigation upon discovering the first remote-access technique, the global criminal group would have been free to continue pillaging the environment. Also, the client asked us to collaborate with law enforcement which created an interactive exchange of evidence that helped us further our investigation and contain the incident and led to the international arrests of the criminals who had used the stolen data to generate millions of dollars in revenue in only a few days after stealing the data.

Corrupt competitors are always looking for an economic advantage by any means.

Corrupt or corruptible users of your IT environment with authorized access to data are the most dangerous threat to private cyber space. The solo artist, or lone wolf, is often one who has fallen on hard times or is a person motivated to achieve revenge due to some unresolved work conflict, perceived or actual potential job loss, or work disenchantment. As such, the insider is also ripe to be recruited by external threat groups, and combined with the economic downturn, we see a fertile and highly exploitable playing field for the recruitment of insiders experiencing financial distress.

Organizations need to enhance pre-employment due diligence for any insider who will have responsibility for IT operations, access to sensitive and protected data, responsibility for electronically transferring money, and other vulnerable functions. Enhanced pre-employment due diligence can often identify those who might be predisposed to committing fraud, theft, or other malfeasance. For certain individuals who have particular job responsibilities, ongoing due diligence might be necessary at predetermined intervals to recognize a brewing credit crisis or other corruptible elements along with enhanced cyber monitoring. We continue to see a steady stream of insider related malicious acts in our investigative work for our clients. Today, there are plenty of external outlets for corrupt insiders to leak information for profit or to public embarrass an employer.

Cyber security—the last decade

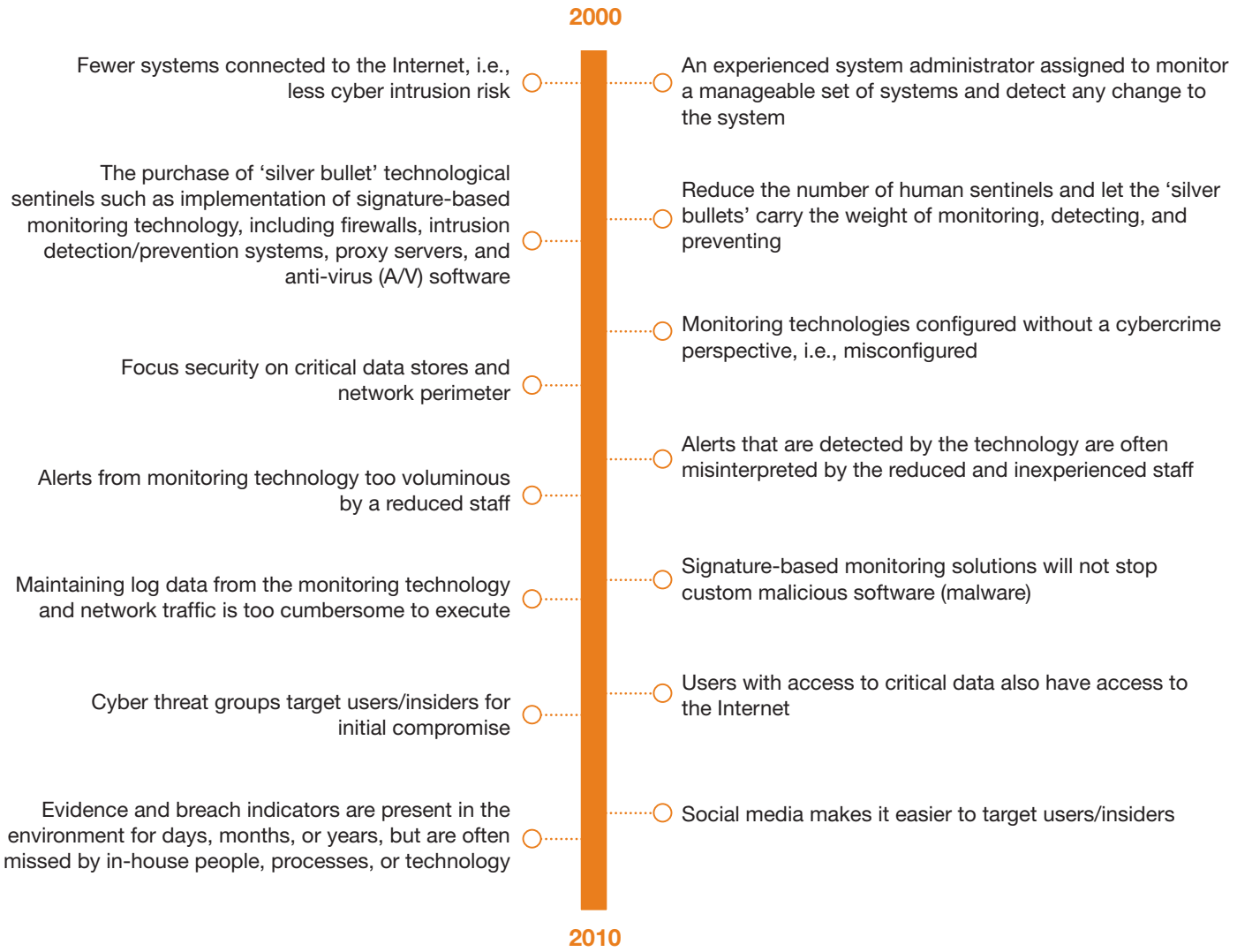
Why do in-house cyber security people, processes, and technology often fail to detect advanced cyber threats designed to maintain remote-access for as long as possible? One reason: The cyber threat landscape is organized, global, highly motivated, sometimes well-funded, patient, and fully immersed in the tradecraft.

A quick journey through cyber security history over the past decade may help spot some additional factors:

The world has found itself with plenty of technological silver bullets and limited experienced human resources with which to combat the cyber threat landscape. It's the artistic side, or the experienced human element, that is desperately needed to raise the level of security by improving the utilization of the security technology.

Wanted: People who have experience in investigating cyber intrusions and who can apply that experience not only to investigating events, but also to think about how to transform all of those silver bullets into advanced warning systems. In our view, investments in security technology over the past decade can still be leveraged to improve cyber security: with the right experience to tune it.

Cybercrime evolution: 2000-2010



Assume a state of compromise

Technological sentinels remain critical assets for managing cyber risk. However, applying a cybercrime investigator's mindset to daily cyber security operations is a much needed capability. Given the cyber threat landscape, the future of cyber security will have to involve human sentinels leveraging technology and custom-developed processes and procedures to constantly interrogate the IT environment forever.

Analogy: A good investigator interrogating the human subject of a fraud investigation will initially spend time to baseline the verbal and nonverbal behaviors of the human subject to enhance the investigator's ability to detect deception. This same concept can be applied to cyber security. Creating a baseline of network traffic and system programs, processes, and connections can greatly assist the ongoing interrogation of the IT environment for breach indicators, because those indicators, or deviations from the norm, can be more readily seen. Stated differently, you can enhance your state of cyber security to become a cyber lie-detector.

Detecting cyber deception requires training, practice, experience, and creativity. Imagine if your nonstop network traffic analysis for breach indicators, which operated from a baseline of known good network traffic, identified a large file being transmitted over a networking protocol that is authorized in your environment but is not used to transmit data. Or, imagine if the ongoing scanning of user systems for breach indicators, which operated from a baseline of known good files, processes, and connections, identified a connection from a user system to an email server in which the user had no email account.

It's time to buid a little rapport with your private space.

Organizations should have a framework for responding to — and *forensically* investigating — cybercrime events. Such a framework should be a high-level guide that enables the organization to adapt to the often fluid events related to cybercrime and empower cyber responders and investigators to collect and analyze evidence effectively so the event can be contained as quickly as possible. An incident response framework should be developed by professionals who are experienced in responding to and mitigating cyber incidents; and personnel must be trained on its execution. Training of these human resources should also raise awareness about the overall strategy of IT security, a review of any independent third-party IT risk assessments, and a review of the business impact analysis from the organization's business continuity management/disaster recovery plan.

Cyber Incident Management Lifecycle

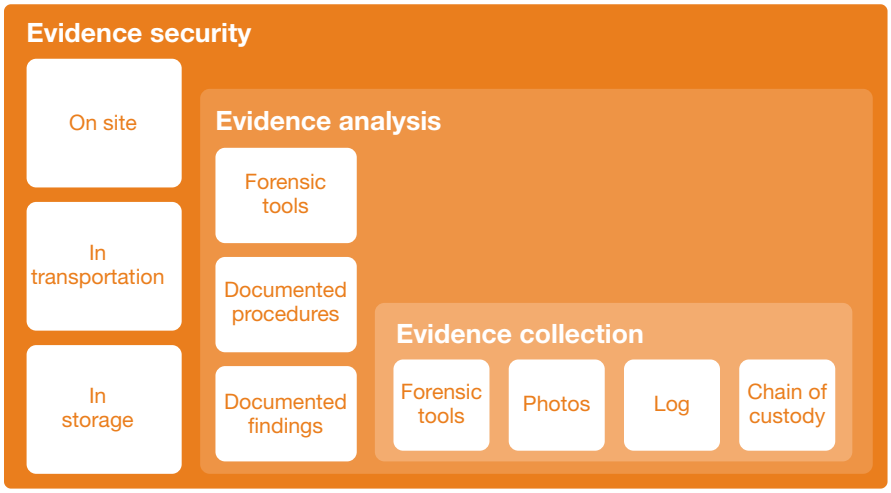
Based on our incident response engagements, here are some common response mistakes we observe when organizations are confronted with a cyber intrusion and/or data theft incident:

- Assigning the organization's IT operations department to investigate the incident: The IT department rarely has employees with the necessary experience to forensically investigate such matters. Further, IT employees have a 'day job;' if they're asked to become investigators, something will suffer—either their routine job responsibilities or the investigation.
- Incident response becomes a technically centric endeavor. As such, key stakeholders who should have insight into the situation often do not, creating organizational risk management blind spots.
- Investigative actions are not forensic. Even organizations that have a dedicated in-house cyber security incident response team (CSIRT) will sometimes perform 'investigative' activities that are not forensic, potentially limiting the organization's ability to defend itself from future regulatory or legal inquiries.

Cyber Incident Management Team

The forensic value of such investigations cannot be underestimated. Numerous critics and organizational risks related to cyber intrusions and data exposure or theft can potentially materialize, ranging from class action lawsuits to regulatory actions. Incident response has to be forensically pure to help manage future unknowns and every activity or task that takes place during an incident should be centrally led, managed, controlled, and documented by seasoned cyber incident leaders.

We recommend that once an incident is contained and security remediation has begun, a formal review of the incident response effort is conducted to assess the team's performance. Results of this review are then used to enhance training and improve future responses. Once all security issues identified during the investigation have been resolved, an independent and objective security assessment should be conducted to confirm successful remediation.



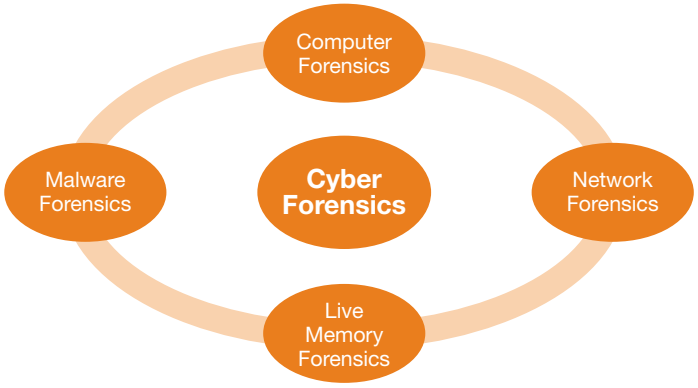
When considering an external forensic service provider to support cybercrime-related events, the technical forensic investigation and supporting cyber forensic capabilities are only one crucial factor. Other capabilities to consider are:

- **Privacy breach notification analysis/support** in compliance with privacy laws for any given country: If personal information or payment card data is viewed, accessed, or acquired, you will likely have to conduct an in-depth analysis on this data to determine the unique instances of an identity or card amongst the entire population of this type of data that was at-risk.
- **Experience in your specific industry** to help understand the other organizational risks.
- **Knowledge of your IT environment** based on past projects or ongoing/periodic projects; this can often dramatically advance how and where to focus investigative efforts and what forensic tools should be brought to bear.

- **Experience working with law enforcement** and government agencies and interfacing with those agencies on your behalf: If government agencies have past experience with your external forensics partner and trust the forensic methods of that partner, they might not need to repeat evidence collection efforts that can disrupt IT and business operations.
- **Testimonial experience:** Should an incident entangle the organization in a legal matter, your forensics partner should be able to articulate its work in manner that will withstand courtroom scrutiny.
- **Deployment of the right resources on a national or global scale:** Having a forensics partner with resources in major business hubs around the world can help reduce response time, overcome language and cultural differences, and provide insight into and understanding of local regulatory and legislative requirements.

Cyber forensics

Cyber incident response requires a variety of forensic capabilities beyond traditional computer forensics. Speed is always essential when investigating suspected cybercrime. The lifespan of digital evidence is short. When a cyber intrusion or data theft incident is discovered, quick response, forensic preservation of digital evidence, and the application of the right analytical methodologies and tools are critical to achieving containment, managing risks, and empowering proper remediation.



"Cyber" forensics is crucial to the investigation cyber security incidents. Cyber forensics includes:

- Computer forensics: the forensic preservation and analysis of computing systems
- Live memory forensics: the forensic preservation and analysis of live memory on systems to identify suspicious or malicious actively running programs
- Malware forensics: the forensic collection and analysis of malicious software (malware) to understand its purpose and capabilities, a process that often speeds up an investigative effort

- Network forensics: the collection and analysis of live and historical network traffic, as well as network monitoring logs to identify suspicious or malicious network-based activity

Let's say an organization identifies a system in the environment that may be compromised. A typical response involves the application of computer forensics, in which the computer in question is analyzed in some manner. But what happens in the absence of evidence of an intrusion or malicious activity on the system being analyzed?

Sometimes malware will be executed by an attacker and running in live memory, but the attacker removes the program from the file system (the focus of computer forensics) or makes the program appear legitimate. Collecting live memory before powering down a suspected compromised system can improve the ability to find malicious activity. Further, live memory analysis can improve malware analysis because if malware is found through computer forensics on a system's hard drive, attackers often use techniques to prevent its analysis. If, however, the malware was running in live memory, it is completely exposed. Not only can the analysis of malware determine the purpose and functionality of the malware, but it can also identify the external systems it's communicating with and other internal systems it has compromised, thereby permitting the investigative trail to continue.

Cyber threat intelligence

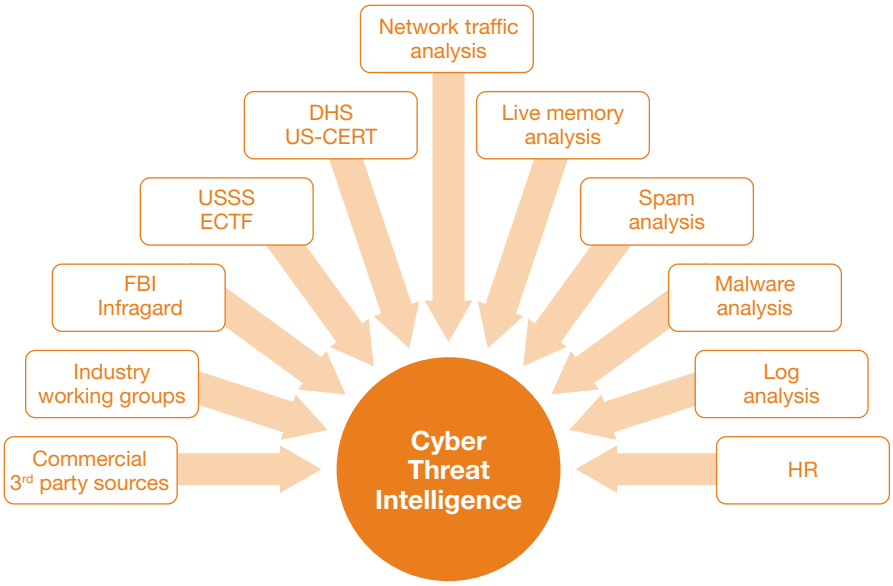
Many organizations today across all industries are discussing how to develop a cyber threat intelligence program. Most companies are also looking to government agencies, for-profit vendors, and free sources for intelligence feeds. However, it's also important to consider the most significant source of cyber threat intelligence: your own IT environment, which can be transformed into a treasure trove of threat intelligence and digital evidence.

Commercial third-party sources include A/V vendors, IDS/IPS vendors, free and pay-for lists of known malicious URLs and IP addresses, free and paid services to determine if your private IP address space is part of a known botnet or other cyber threat.

Industry working groups (people from various organizations with the same industry), in which cyber threat intelligence is openly shared but is not available to the general public, can be found.

Government agencies have also established vehicles for sharing cyber threat intelligence:

- **Infragard** was started in the late 1990s as a partnership between the FBI and the private sector. It aims to share information by combining the knowledge base of the FBI, businesses, academic institutions, state and local law enforcement agencies, and others who are committed to sharing information and intelligence to prevent hostile acts against the United States.



- As a result of the 2001 USA Patriotic Act, the United States Secret Service (USSS) was mandated to establish a nationwide network of **Electronic Crimes Task Forces.** These task forces are compromised of the USSS, businesses, academic institutions, state and local law enforcement agencies, and others focused on electronic crimes against financial institutions.
- The **United States Cyber Emergency Response Team** (US_CERT) was formed by the Department of Homeland Security in 2003. Its mission includes the sharing of cyber security information with state and local governments, industry, researchers, and the public.

Leading practices

In the future, cyber security will have to integrate all of these intelligence sources in a state of perpetual analysis to enhance and safeguard operations:

Network traffic should be collected at every Internet-access point and maintained as a part of the data backup strategy. The ability to have access to historical network traffic can significantly enhance incident response efforts by enabling you to determine the root cause and duration of the compromise. Real-time network traffic monitoring technology should be configured by resources who understand the methods used by the cyber threat landscape to empower a more effective alert system. In addition to collection and monitoring traffic to and from the Internet, consideration should also be given to monitoring critical internal data storage locations.

Custom malware that is not publicly known will not have a signature that can be used up by signature-based detection and prevention technologies. Organizations need a systematic and scheduled method for gathering live memory from internal systems to identify suspicious programs and associated behaviours. This is an emerging and necessary capability, and, for the time being, live memory just may be the last stand on the cyber battlefield.

For any malware specimen discovered in private cyber space, there is a serious need to fully understand the capabilities of the malware and to use that intelligence to interrogate the environment further for breach indicators and enhance security controls. The standard approach of letting A/V software remove the malware and then let IT rebuild infected systems only creates more cyber security blind spots. The availability of an internal capability or outside partner to analyze malware can catapult a cyber security posture to new levels.

Organizations also need to consider that malware typically gets delivered by way of email messages containing malicious links or attachments. Therefore, it makes sense to analyze spam and spear phishing messages, which in turn can become a critical component of cyber threat intelligence. These messages have to be analyzed quickly because the Internet-related aspects of malicious links or attachments are active only for a very short time.

Analyzing logs from firewalls, IDS/IPS, A/V, proxy servers, operating systems, and the like is certainly an important element of cyber forensic investigations. Most cyber investigators would agree that these logs may not be properly maintained and often lack sufficient useful information. Technologies should be configured to log activity that is useful to incident response; logs should never be overwritten; and they should be a part of the data backup program. On the proactive front, some organizations are leveraging log aggregation technology to gather logs in a central location for more effective analysis. However, the end-point technologies are often not configured to capture the right suspicious activity, or the log aggregator is not configured properly to alert on suspicious activity, or the alerts are misinterpreted by a reduced and inexperienced staff. Logs have to be aggregated in a way that permits a security analyst who understands the cyber threat landscape to continually interrogate the logs with innovative methods to find the breach indicators.

Remember that insiders can also pose a threat to private cyber space, whether their goal is to steal data for financial gain, leak data to outsiders for financial gain or damage the organization's reputation, or disrupt IT services and impact business operations. The underlying motives typically can be classified as:

If the human resources department, ethics office, or any other internal source identifies these risk factors, then the organization can implement enhanced cyber monitoring of insiders who have sensitive job responsibilities or access to sensitive data for unauthorized behavior to better prevent or detect data theft or leakage.

What this means for your business

A new cyber security philosophy

Mature cyber security programs are typically comprised of numerous complementary elements, including security management, operations, and architecture; regular testing for compliance with regulations; established policies and procedures; privacy; education and awareness; identity and access management; threat and vulnerability management; physical security; and incident response.

Even mature cyber security programs can benefit from a new cyber security philosophy to improve the security of data and the IT infrastructures that contain it. This philosophy includes the recognition that there are no silver technological bullets. Rather, the approach assumes an active and perpetual state of compromise, seizes all opportunities to gather cyber threat intelligence, transforms the IT environment into a treasure trove of digital evidence, assesses the state of security of its interconnected vendors, recognizes the authorized insider as a cyber threat, has a forensic incident response capability, and understands and overlays business operations needs—all in an effort to fuel an enhanced state of cyber security.

Historical cyber security

Use signature-based monitoring technology such as firewalls, intrusion detection/prevention systems, proxy servers, and anti-virus (A/V) systems to detect suspicious activity.

- Reduce the number of human staff.
- Focus detection on critical data stores and network perimeter.
- Minimize logging on user systems.
- Let A/V software secure user systems.
- Let IT configure monitoring technology.
- Let IT investigate suspicious events.
- Treat security assessments as a series of one-time events, or 'checking a box.'

Emerging cyber security

- Enhance signature-based technologies with custom rules and alerts informed by a cybercrime mindset.
- Collect and maintain all logs from monitoring technology and systems.
- Focus detection on all systems, not just on critical data stores and external-facing computers.
- Increase operating system logging on all systems.
- Have a systematic method to collect and analyze live memory on systems.
- Collect and maintain all network traffic.
- Minimize Internet-access points.
- Baseline network traffic.
- Use a limited set of system configurations and baseline them.
- Analyze all phishing emails.
- Analyze all malware.
- Have a cyber incident response framework that relies upon experienced cybercrime and cyber forensics resources.
- Have an all source cyber intelligence program.
- Have an ongoing security assessment program and immediately address areas of risk.
- Have a program to assess and identify high risk insiders.

Cybercrime and those who commit it are always evolving, focused on accessing your sensitive information and maintaining persistent remote access for as long as they possibly can. The cyber threat landscape is committed to deeply understanding your IT environment in order to achieve the objectives of the cyber intrusion. Companies that want to better protect themselves and their stakeholders from advanced cyber threats will have to adopt this new cyber security philosophy: a philosophy that will be central to enhancing security for years to come.

www.pwc.com

To have a deeper conversation about how this subject may affect your business, please contact:

Shane Sims
Director
PwC
703 918 6219
shane.sims@us.pwc.com

Kimberly Peretti
Director
PwC
703 918 1500
kimberly.k.peretti@us.pwc.com

Ed Gibson
Director
PwC
703 918 3550
ed.gibson@us.pwc.com

David Burg
Principal
PwC
703 918 1067
david.b.burg@us.pwc.com