



# EXECUTIVE SUMMARY

Information is the lifeblood of many organizations, and thanks to modern computing technology, that information can be easily shared with colleagues, clients and suppliers. As our dependency on computers and technology deepens, so do the risks and threats to those systems. These threats range from curious teenagers to disgruntled employees, activists, criminals, industrial and state sponsored spies, terrorists and even nation states engaged in warfare.

To ensure the security of a company's business-critical information, it is essential to develop a cohesive multi-layered strategy to address the threats. Traditionally, organizations focus their defensive controls at the perimeter in the belief that this makes it difficult for attackers to penetrate systems. However, once this perimeter is breached, the attackers have relatively free reign within the network. Hardened, perimeter defenses alone also fail to manage the threat from internal sources.

Organizations need to develop a multi-layered security strategy that focuses on the confidentiality, integrity and availability of the information being protected. A multi-layered approach to security ensures that if one layer fails or is compromised, other layers will compensate and maintain the security of that information. In turn, each of these layers should have multiple controls deployed to preserve the confidentiality, integrity and availability of the information. Some of these more critical controls include system configuration hardening, file integrity monitoring, and log management.

This paper will examine the various threat sources of protected information, along with the different security layers and controls that can be implemented to tackle those threats. It also discusses the dependencies and sources of failure to consider when implementing these layers and controls, and how to prioritize them.

## EVOLUTION OF THREATS

Ever since computing began systems have been under threat, either by those with malicious intent, or from mistakes by well-intentioned people. As the business use of computers evolved over the years, so have the threats facing them.

Initially, external threats were limited predominantly to those interested in breaking into computer systems out of curiosity to determine how computers worked. In the majority of cases, the motivation was curiosity and fame, not malicious intent.

The introduction of personal computers and the Internet resulted in much greater data sharing, which allowed organizations to be more effective and communicate better with their customers. While the threat posed by those who were simply curious still

remained, a new threat emerged from those motivated by financial gain. This new group saw the explosion of systems onto the Internet as an opportunity to make money by exploiting weak system security. Others saw the Internet as a medium for activism and attacked systems to gain notoriety for their cause, mainly by defacing websites of organizations with which they did not agree.

The explosion of the Internet as a platform for commerce in the first decade of the 21st century added a new threat. Organizations now store and transmit ever-increasing amounts of sensitive data on their computer systems, including confidential company information, customer data, credit card information or intellectual property. Just as computers and the Internet provide organizations opportunities to reach new markets, they also provide organized criminal gangs new opportunities to exploit weak security. These gangs often reap financial gains with little risk of being prosecuted.

Computer viruses and other malware have also evolved over the past decades. Although the first computer viruses were relatively benign, over the years they have grown more sophisticated and destructive. Today malware is a major tool in the arsenal of computer criminals and other threat actors.

Just as computers and networks have evolved to enable organizations to be more productive, so have the threats. The traditional insider threat still remains, and as technology progresses, so have the knowledge, capabilities, sophistication and profiles of the external threat sources. Understanding what you are trying to protect and your threat sources is critical to deploying the critical controls that protect against those threats.

∴ Hardened, perimeter defenses alone also fail to manage the threat from internal sources. ∴

# THREAT SOURCES

Threats to information security can come from many sources. Generally threat sources can be split into two main categories: external and internal sources. External threat sources can range from state-sponsored foes to industrial espionage, organized criminals, and individuals hacking out of curiosity or activism. Internal threats can come from employees or contractors with malicious intent.

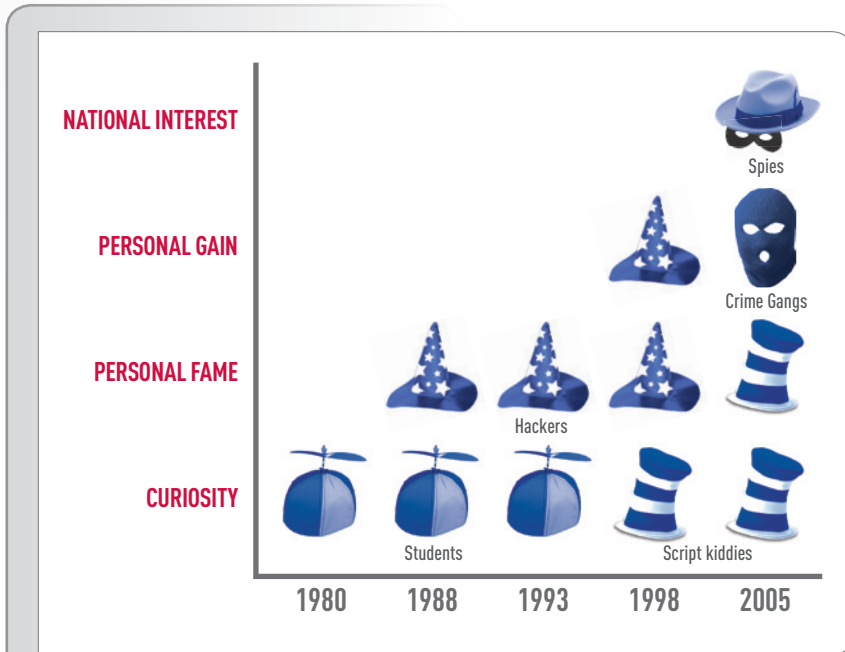


FIG. 1 The evolution of threat sources

Any organization will face a variety of types of threats, some more serious than others. For example, an organization working on government defense contracts will face different threats than a small local business with a website with no e-commerce capabilities. An online retailer processing thousands of credit card details will face different threats than a news website.

## EXTERNAL THREAT SOURCES

Numerous external threat sources can impact on the security of your information and systems. While attackers can

be categorized into different groups, some attackers can be in more than one group, while others may move from one group to another as their skills and motivations evolve. External threat sources can broadly be categorized into the following groups:

### EXTERNAL TARGETED THREAT SOURCE

#### » FOR PROFIT

Predominantly driven by criminal groups, for-profit threats focus on making money through their activities. Activities range from extorting money

from system owners by threatening to take their systems off line, to breaking into systems to steal financial information—the organizations' own online banking systems or financial information of customers, such as credit card information. The infamous TJX breach is an example of such a threat.<sup>1</sup>

#### » CHAOTIC

Those motivated by a cause will use their technical skills to attack websites and systems of organizations they have a grievance with. These attacks can range from defacing websites or breaking into systems to steal information that could embarrass the target organization. Others attack organizations simply for thrills and entertainment. Anonymous and Lulzsec are prime examples.<sup>2</sup>

### STATE SPONSORED

State-sponsored threats generally have much greater funds and more resources than other threat sources, and as a result they are harder to defend, detect and respond to. Some nation states may also engage criminal gangs to carry out their attacks to provide a certain level of plausible deniability should the attack be detected. The two main threat sources in this category are:

#### » STATE SPONSORED ESPIONAGE

Hostile nations will attempt to break into the computer systems of foreign governments, or contractors working for that government, to steal sensitive information.

#### » STATE SPONSORED ATTACKS

Hostile nations may also directly attack against computer systems of a target government. In wartime, attacks may be against military or civilian targets, with the aim to disrupt or cause those systems to fail. Attacks may also break into a target country's systems to spread false information that results

in confusion and chaos. The development of tools, or cyber weapons, to enable such attacks is a key concern. Although no government or group has been assigned responsibility for the Stuxnet worm<sup>3</sup>, many speculate that it was a state-sponsored attack because it was aimed at the Iranian government's plutonium enrichment program.

**EXTERNAL OPPORTUNISTIC THREAT SOURCE**

While certain attacks from external sources are aimed at specific organizations, many other attacks are simply opportunistic with no, distinct target. These threats are:

» **MALWARE AND BOTNETS**

Modern malware, such as viruses, worms and Trojans, is typically not written with a specific target in mind. Rather, these attacks aim to infect as many computers as possible to steal sensitive financial data such as credit card information. They may also be aimed at creating a network of computers (a botnet) that criminals can control.

Botnets provide criminals with the ability to industrialize their efforts, allowing them to:

- » Perform DDoS attacks against a target system and demand payment from the system owner to prevent further attacks;
- » Send spam emails promoting activities the criminal gang may be involved in, such as pharmaceutical goods, adult websites or other illegal or immoral items;
- » Send phishing emails to customers of financial institutions in order to harvest their financial details; or
- » Spread other malware to the infected systems or to infect other systems to increase the size, and therefore capability, of the botnet.

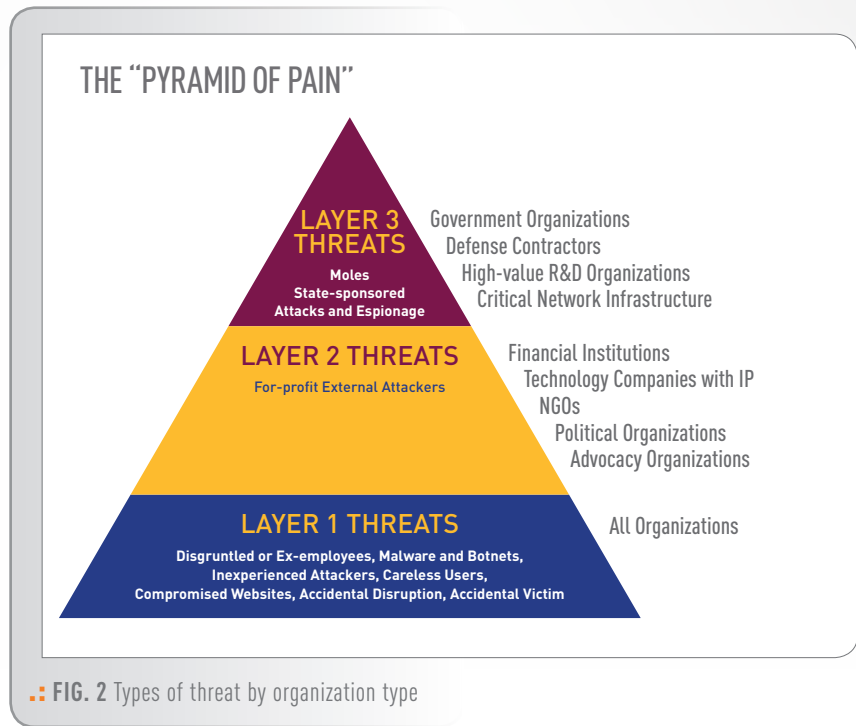


FIG. 2 Types of threat by organization type

Criminal gangs also provide their botnets for hire, enabling those without the technical skills to easily get involved in online criminal activity.<sup>4</sup>

» **COMPROMISED WEBSITES**

Criminals will often break into the websites or systems of unsuspecting organizations to host their phishing sites, spread malware to unsuspecting users visiting that site, or store and distribute illegal material. These websites will not be noticeably altered, as the longer the compromise goes undetected, the longer the criminals can use the site to carry out their activities.

» **INEXPERIENCED ATTACKERS**

Not all attackers have sophisticated computing skills. Those less technically capable can download and use tools

developed by more skilled attackers. Their indiscriminate use of these tools and lack of technical knowledge means that this type of attacker (derisively referred to as a "script-kiddie") can potentially, and often unintentionally, cause damage to systems despite their inexperience.

**INTERNAL NON-MALICIOUS THREAT SOURCE**

Many employees in an organization do not wish to cause any damage or harm to the systems they use as part of their day-to-day jobs. Most simply use computers as a tool to help them get their job done. Sometimes however, even the most well-intentioned employee can pose a threat to the security of an organization's system.

» ACCIDENTAL DISRUPTION

Users who are not trained or unfamiliar with a certain system may mistakenly alter or delete information unintentionally. For example, they could delete a file or files on a server or corrupt system information by overwriting or altering certain files.

» ACCIDENTAL VICTIM

Employees may visit websites laced with malware that the site's owner or a criminal added. The malware, which has been designed to exploit bugs or vulnerabilities in browsers, inadvertently gets downloaded onto and infects vulnerable computers.

In other cases an external attacker may dupe the employee to click a link in an email or provide their logon credentials over the phone, which results in the attacker gaining access to the organization's systems.

» THE CARELESS USER

Some users will compromise systems by simply not following or ignoring the advice they have been given in how to perform their role securely. This could range from sending confidential information over insecure channels such as email, downloading sensitive information onto portable media such as a CD or USB key, losing a laptop, or writing down their logon credentials on a piece of paper.

**INTERNAL MALICIOUS THREAT SOURCES**

The malicious insider threat is one that can cause the greatest damage, as the insider is a trusted individual with access to systems containing sensitive data and in-depth knowledge of the weaknesses in those systems. Jérôme Kerviel, a junior equities trader in Société Générale who caused a loss of \$7.2 billion in 2008 illustrates a prime example of an internal threat.

Generally the malicious insider can be broken into three categories:

» THE MOLE

The mole is an individual who has targeted a specific organization by becoming a member of staff, or for a company contracting with the target organization, with the sole purpose of gaining access to sensitive information or disrupting systems. Typically this type of threat source targets government agencies, private companies working on sensitive government contracts, or organizations developing solutions with high-value intellectual property.

Alternatively the mole may be an existing employee who is persuaded by someone else, either by coercion or bribery, to compromise sensitive systems or information.

Due to the high-risk nature of being caught and the value of the targeted systems, a mole is typically sponsored or supported by a well-funded adversary such as a nation state, organized crime or an aggressive competitor.

» DISGRUNTLED EMPLOYEE

An employee may become disgruntled for a variety of reasons. In retaliation for perceived slights, the employee may attempt to steal information (in order to sell it to interested third parties) or seek revenge by destroying data or shutting down systems, as in the case of a UBS employee in 2002.<sup>6</sup>

It's also possible that some employees who are either in the process of leaving the organization, or feel their role is under threat through redundancy or mergers, will copy sensitive data to use in their new place of employment or sell to others.

» FORMER EMPLOYEES

Another form of disgruntled employee is the former employee who may feel aggrieved because their employment was terminated. However, in some cases the former employee's system access may not be revoked or they may know and use the logon credentials of a former colleague to remotely access and compromise the systems and information. An example of such an attack is that of a former employee of Gucci America.<sup>7</sup>

∴ Understanding what you are trying to protect and your threat sources is critical to deploying the critical controls that protect against those threats. ∴

# SECURITY LAYERS

Relying on a single security layer is no longer prudent in today's threat landscape. Organizations need to focus on the information they are protecting and build layers of security around it. In effect, they need to create a defense-in-depth solution.

SECURITY LAYER	PREVENTATIVE CONTROLS							DETECTIVE CONTROLS						
	User Access Control	Network Access Control	Encryption	System Hardening	Software Patching and Updates	Malware Detection/Prevention	Security Awareness Training	Policies & Procedures	Change Control	Security Configuration Management	Log Monitoring	File Integrity Monitoring	Vulnerability Management	Incident Alerting
Physical Layer			✓	✓			✓	✓	✓					✓
Network Perimeter		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
Local Area Network		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
Wide Area Network		✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
Virtualization Hypervisor	✓			✓	✓	✓			✓	✓	✓	✓	✓	✓
Virtualization Virtual Network	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓
Host System	✓			✓	✓	✓			✓	✓	✓	✓	✓	✓
Application	✓			✓	✓	✓			✓	✓	✓	✓	✓	✓
Intellectual Property	✓		✓								✓	✓		✓
Entrusted Data (e.g. PII)	✓		✓								✓	✓		✓
Sensitive Databases	✓		✓								✓	✓		✓
Sensitive Files	✓		✓								✓	✓		✓

FIG. 3 Typical security layers organizations should consider

## DEPENDENCIES/SOURCES OF SECURITY FAILURES

As previously mentioned, many organizations focus their security controls on the perimeter of their networks. When those controls are breached, the attackers have relatively easy access to sensitive systems and data within the network. This is commonly known as “M&M security,” as the security structure of the system is similar to M&M candy—hard on the outside, but soft on the inside. Once the attacker has breached the hard

perimeter and is inside the network, they gain access to any number of systems because they are now viewed as a trusted user—or are completely invisible to the organization.

When an organization focuses its security controls on one layer of protection, such as the perimeter layer, its entire security can be dependent on those controls working effectively at all times against all threats. Should one of those controls fail, the entire security layer

can be bypassed. Given today's threats, security professionals need to build security in defensive layers so that if one layer is breached, the other layers continue to provide security. Many security breaches are the result of incorrectly configured systems, out-of-date software patches, inappropriate user access permissions, lack of awareness of the security threats, or inadequate policies, processes and procedures.

Often an information security management system fails when individual controls fail and no other controls are in place to monitor, detect and/or compensate for that failure. This situation is exacerbated when those controls are developed in isolation; in such cases, they provide no overlapping protection and cannot communicate with each other. Without the ability to monitor the effectiveness of their security controls, organizations cannot even determine if the controls are appropriate. Without monitoring, an organization also won't know when they have suffered a security incident. This in turn can lead to ineffective incident response, as the organization does not know the source, target or extent of the breach.

Clearly organizations must take a layered approach when designing their security system. This approach should ensure it protects the confidentiality, integrity and availability of that information. It should also ensure that all security controls are integrated and focused on managing the various levels of risk posed against key information and systems. Focusing on controls such as firewalls, anti-virus software or other technical controls is not the answer. More technology will not secure the information; a combination of better management and the right technology will.

## APPROACHES TO PRIORITIZATION

Implementing a layered security program is similar to implementing any other business initiative: executives contend with a lack of staff and budget and therefore cannot implement everything they want. Therefore, organizations must take a risk-based approach to identifying and implementing the various information security controls, and should focus on the information being protected.

The following steps are key for developing this risk-based approach:

### STEP 1: IDENTIFY KEY INFORMATION

The adage “you cannot protect what you do not know” is especially true in information security. Therefore, the first step is to identify what information is important to the organization and where that information is located.

### STEP 2: CATEGORIZE INFORMATION

Once identified, the information should be categorized in accordance with its importance to the organization. This importance can have a monetary value or an abstract valuation based on the impact the loss of that information would have on the organization’s business operations or reputation.

### STEP 3: IDENTIFY THREATS

The organization should next look at the various threats—and source of threats—that are posed against the identified, and now categorized information. For example, a government-funded threat source will pose a greater threat than a casual attacker. Whether an organization needs to worry about government-sponsored attacks will be dependent on the nature of their business.

### STEP 4: ASSESS VULNERABILITIES

Once the threats have been identified, the organization should next identify vulnerabilities in existing security controls and ascertain the likelihood that they will be exploited. For example, a vulnerability that is technically difficult to exploit is potentially of less concern than an easily exploited one.

### STEP 5: ASSESS THE RISKS

Once the above has been ascertained, the information security risks posed against the organization can be determined by examining the various threats, their sources, the likelihood of a threat materializing, and the impact a threat will have on the protected information. These risks can then be categorized based on their potential impact to the organization. By following this process, an organization can then prioritize what risks require additional security controls to better protect its information and systems.

### STEP 6: IDENTIFY CONTROLS

At this point, the organization can identify what specific security controls it needs at the various layers to ensure all risks are at a level acceptable to the business. Begin by identifying controls that address the highest rated risks. The focus should start with the controls at the information layer, proceeding to the controls needed at the various outer layers. But beyond the implementation of technical controls, the organization must ensure that proper policies, processes and procedures are in place and adhered to. Such adherence may require training of personnel.

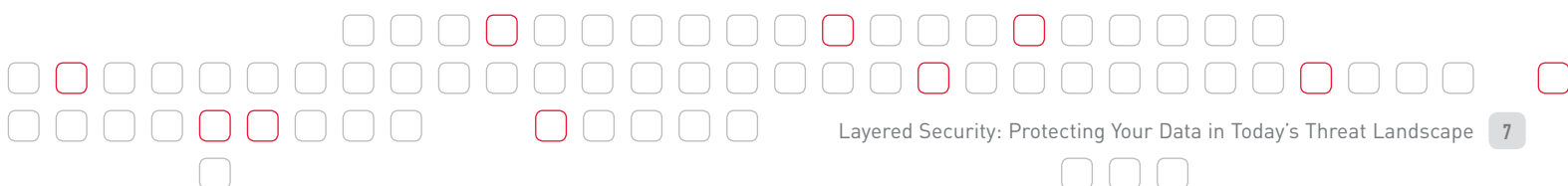
### STEP 7: IMPLEMENT CONTROLS

The organization should now begin implementing the controls, ensuring a layered approach is taken so that if one control fails, the organization is aware of the failure and other controls can compensate. As controls are implemented, they should be tested to verify that they both work as planned and address the risk they are supposed to manage.

### STEP 8: MONITOR CONTINUOUSLY

Over time business requirements change, new systems are added to the network, and the technology used on systems changes and gets updated regularly. As such, it is important that this risk-based approach be a continuous process that evolves with the business. Learning from past mistakes and identified weaknesses in the security controls, whether from people, process or technology, will enable the security controls protecting critical assets to mature in line with the business’s requirements.

∴ Focusing on controls such as firewalls, anti-virus software or other technical controls is not the answer. More technology will not secure the information; a combination of better management and the right technology will. ∴



# LAYERED SECURITY CONTROLS

Numerous security controls can be implemented when an organization is designing a multi-layered security infrastructure. These controls generally fall into preventive and detective categories.

## PREVENTIVE SECURITY CONTROLS

The following are some of the main preventive controls that an organization should consider:

### MALWARE DETECTION/PREVENTION

Given the high prevalence of malware, all computer systems should have software installed that identifies and prevents it. It is equally important to ensure that the anti-malware software is kept up to date so it can prevent the latest versions of malware from attacking the systems.

### SOFTWARE PATCHING AND UPDATES

Keeping critical software patched and up to date makes it more difficult for attackers to break into those systems. Therefore it's critical to consistently update systems with the latest software releases and patches.

### SYSTEM HARDENING

Typical default configurations for most applications and operating systems enables them to work in the majority of environments. However, these generic configurations are often the least secure, so systems should be hardened. This process involves taking steps such as removing default user accounts and passwords, removing unnecessary services, and adjusting permissions.

### USER ACCESS CONTROL

The access rights set on systems and other resources should reflect the level of access different users require to conduct their jobs. For example, people in sales and marketing do not need access to the payroll system. Likewise, within the payroll system a manager should

have a different access level than an administrative person.

### NETWORK ACCESS CONTROL

How systems access the network should be strictly controlled. This can be done by isolating sensitive systems from the main network into dedicated secure segments, with access to those network segments controlled via firewalls configured with strict access rules. Perimeter defenses should include mechanisms such as firewalls, intrusion detection systems and network traffic filtering.

### SECURITY AWARENESS TRAINING

It is important to train employees so that they are fully aware of the risks and threats posed against the systems

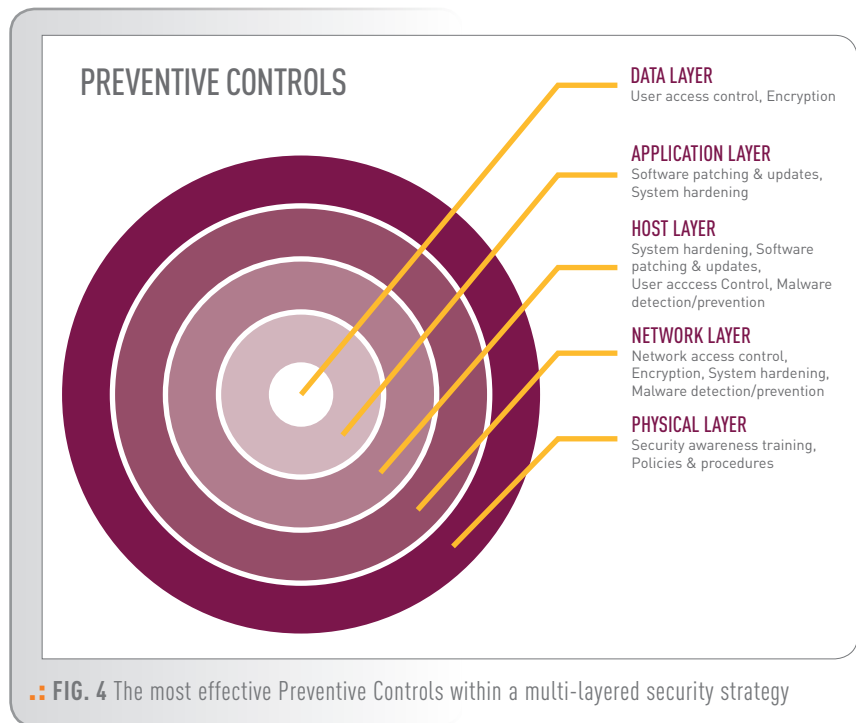
and information they use. It is equally important to ensure they understand the security controls that are in place. Particular focus should be placed on training users on how to recognize attempts to elicit sensitive information from them via emails, phone calls or other means.

### POLICIES AND PROCEDURES

Well-written, clear and concise policies and procedures help ensure that everyone is fully aware of the importance of implementing the various security controls, each user's role in ensuring those security controls are effective, and the consequences of those controls being ignored or bypassed.

### ENCRYPTION

Encrypting sensitive information, whether it is at rest or in transit, can ensure that only authorized personnel have access to it. Should the encrypted information be copied or stolen, it will be unreadable and therefore of no value.





# SUMMARY

In today's business world, information is the key to success. Yet now more than ever, that information faces threats to its security. For this reason, it is essential that information be secured so that it is only available to those authorized to access it. This increasing threat environment, coupled with a more interconnected world, mobile and remote workforces, and ease of information sharing means our traditional perimeter-centric view of security is no longer valid. There is no a single perimeter or layer behind which all things are secure.

The evolving nature of the security threats many organizations face requires organizations to cease their reliance on a single layer of security to protect their sensitive data and systems. Instead, a multi-layered approach needs to be taken—one in which the security controls are selected and implemented with information as its core. This approach should also ensure that the selected controls are integrated to enable the organization to better visualize and manage potential threats.

In turn, this will ensure that the organization can obtain and act on more accurate intelligence to better manage business risks.

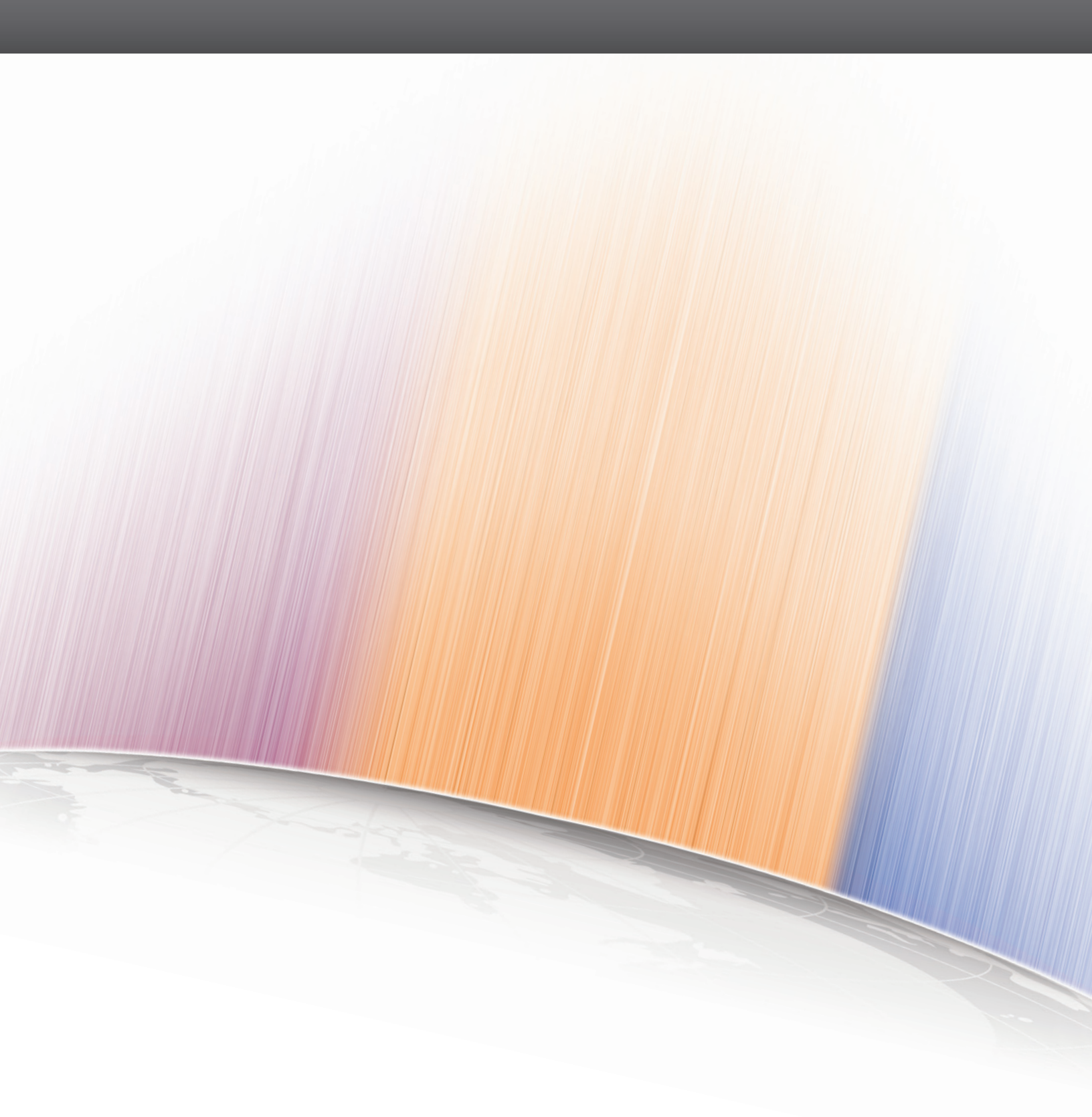
Now more than ever, information security can no longer be a set-and-forget solution, but instead needs to be effectively developed, thoughtfully implemented, and continuously managed. Only then can organizations have confidence that the information that they and their customers rely on is protected.

# ABOUT BRIAN HONAN

Brian Honan is an independent security consultant based in Dublin, Ireland, and is a recognized as an information security industry expert. He has addressed a number of major conferences relating to the management and securing of information technology, such as RSA Europe, BruCON, Source Barcelona and numerous others. Brian is COO of the Common Assurance Maturity Model and founder and head of IRISSCERT, which is Ireland's first CERT. Brian also

sits on the Technical Advisory Board for a number of innovative information security companies, and is on the board of the UK and Irish Chapter of the Cloud Security Alliance. Brian is author of the book "ISO 27001 in a Windows Environment", is regularly published in a number of industry recognized publications, and serves as the European Editor for the SANS Institute's weekly SANS NewsBites, a semi-weekly electronic newsletter.

- 1 <http://www.wired.com/threatlevel/2010/03/tjx-sentencing/>
- 2 <http://www.pcmag.com/article2/0,2817,2387396,00.asp>
- 3 [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)
- 4 [http://www.msnbc.msn.com/id/43978739/ns/technology\\_and\\_science-security/](http://www.msnbc.msn.com/id/43978739/ns/technology_and_science-security/)
- 5 <http://www.ft.com/intl/cms/s/0/e50df9b4-d613-11dc-b9f4-0000779fd2ac.html#axzz1UTcuS0nl>
- 6 <http://www.independent.co.uk/news/business/news/disgruntled-worker-tried-to-cripple-ubs-in-protest-over-32000-bonus-481515.html>
- 7 <http://online.wsj.com/article/SB10001424052748703712504576243312850500374.html>



• Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. •

LEARN MORE AT [WWW.TRIPWIRE.COM](http://WWW.TRIPWIRE.COM) OR FOLLOW US @TRIPWIREINC ON TWITTER.