California data breach

Failure to use basic security measures -- such as encrypting sensitive personal information is cited for putting 1.4 million Californians at risk.

"People are afraid of encryption because they think they need to understand the actual encryption part of it, when in fact you don't."

In reality "there's no good evidence that good encryption programs can be broken. "In the future, the default data state needs to be encrypted."

Understanding Advanced Cyber Threats

Online advertisements are 182 times more likely to deliver malicious content than pornographic sites.

The common notion that illegal or malicious sites expose you to the most risk is outdated. The vast majority of web malware encounters happen on legitimate and trusted websites that you already visit.

Cyber Espionage

A mysterious group of computer hackers has spent four years spying on the South Korean military.

A dangerous cyber espionage campaign, Net-Traveler, has also been uncovered.

The Red October attack campaign is the latest example of advanced forensics efforts leading to new and fascinating revelations.

"Enterprises that haven’t embraced the importance of anti-phishing, strong authentication, rapid patching and network monitoring will be successfully exploited."

IT managers ignore corporate network vulnerabilities

Global ICT solutions and services provider Dimension Data says that the number of devices on corporate IT networks carrying vulnerabilities has dropped from 75% in 2011 to 67% in 2012.

It highlights the on-going 'lax approach' to security on the part of network managers.
FROM THE DESK OF ECS-CSIRT...

The Cost of Lost and Stolen Devices

- 70 million smartphones are lost each year – only 7% are recovered
- 36% of tablets contain confidential work-related information
- 50% of all mobile device users keep passwords, personal information and credit card info on their device

A stolen or lost mobile device with unprotected storage allows an attacker to access the data on it. If the device is infected with malware, it may lead to hidden use of premium services, or leaking sensitive information.

SIM swap fraud

Following a recent spate of SIM swap banking fraud, the South African Banking Risk Information Centre (Sabric) – together with mobile operators and law enforcement entities – is working to combat cybercrime and spread awareness.

Sabric has urged SA’s consumers to adopt stricter personal IT security measures and, as part of its education campaign on SIM swap fraud and the rising threat of phishing, has issued tips to avoid falling victim to crime.

Security for a Faster World

As cyber-crimes become increasingly advanced, pervasive, and costly, organizations are pondering how secure their enterprise really is.

Although far from a new threat, cybercrime is getting increasingly sophisticated, often nipping at the heels or surpassing the security of enterprises. Security tools and programs are constantly evolving to meet the new challenges, and security planning is no longer just an annual event. As attack methods change, so too must defence strategies if they are to stay ahead of the curve.

How secure are you? How much security is enough? Although it is important to meet compliance requirements and secure the perimeter, remember that threats are constantly evolving. As the adversaries become more sophisticated, so must your capabilities.

Windows XP security updates ending

Microsoft will end support for its Windows XP operating system. XP still runs on about one out of every four corporate PCs.

If XP is still running on so many corporate systems a year from now when regular software security patches stop coming, hackers will likely ramp up attacks on the OS beyond the frequent penetration seen today, putting corporate networks in greater danger.

RECENT ECS-CSIRT ADVISORIES

<table>
<thead>
<tr>
<th>Date</th>
<th>Advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Sep 2013</td>
<td>Microsoft Security Bulletin Summary for September 2013</td>
</tr>
<tr>
<td>3 Sep 2013</td>
<td>Microsoft Security Bulletin Summary for August 2013</td>
</tr>
<tr>
<td>2 Aug 2013</td>
<td>Multiple Cisco products are affected by a vulnerability</td>
</tr>
<tr>
<td>1 Aug 2013</td>
<td>Security updates available for Adobe Digital Editions</td>
</tr>
</tbody>
</table>

"10% of laptops are lost over the lifetime of the device."

"There's certainly the potential for a lot of havoc."
Data breaches in California exposed more than 2.5 million residents to the risk of identity theft in 2012, according to a data breach report by the California Attorney General's Office.

Failure to use basic security measures -- such as encrypting sensitive personal information, including social security numbers, credit card and bank account information, medical and insurance data, and driver's license numbers -- is cited for putting 1.4 million Californians at risk with these breaches.

What's behind this failure to encrypt? "Cryptofear," said John Kindervag, vice president and principal analyst for Cambridge, Mass.-based Forrester Research Inc. "People are afraid of encryption because they think they need to understand the actual encryption part of it, when in fact you don't. You just need to understand the processes and the management. The word 'encryption' still scares people, even though it's a mature technology and can solve a lot of problems."

Movies, such as Skyfall, don't do encryption any favours by making it look as if it can be easily broken, when in reality "there's no good evidence that good encryption programs can be broken -- even by the NSA," Kindervag said. "In the future, the default data state needs to be encrypted."

"In the future, the default data state needs to be encrypted."

Better ways to protect against insider data breaches?

More than half (55%) of the California data breaches were the result of deliberate intrusions by outsiders or unauthorized insiders, which begs the question: Is there a better way to protect against insiders in these breaches?

The California breach report is "a wake-up call to every company and government organization that stronger security is needed to protect against both insider threats and breaches," said Eric Chiu, president and founder of HyTrust, a Mountain View, Calif.-based cloud control company. "As we just saw in the Snowden incident, the stakes are high and can ultimately damage the company's brand, impact shareholder value and put jobs on the line."

Breaches frequently target stealing valuable, embarrassing, confidential or customer data to sell on the open market or to go to the public with. These attacks "generally involve insider threats or attackers posing as insiders," Chiu said. "Most companies do an appalling job of securing access to data once you're inside the organization. This needs to change. Companies should assume the bad guys are already inside and put in place fine-grained access controls to restrict access to sensitive data, as well as role-based monitoring to detect when bad things are happening."

Understanding Advanced Cyber Threats

Expanding connectivity from any device to many clouds is having a significant impact on the threat landscape. As more people embrace multiple devices that connect to various networks and services through a wide range of applications, more vulnerabilities are exposed. Delve into the security threats and challenges of 2012 with analysis from Cisco's global threat intelligence.

Highlights of the Report:

Android malware grows 2577% over 2012; mobile only makes up 0.5% of total web malware encounters.

Online advertisements are 182 times more likely to deliver malicious content than pornographic sites.

Global spam volumes are down 18% overall, with spammers keeping banker's hours for a 25% drop over the weekend.

Threats in Plain Sight

The common notion that illegal or malicious sites expose you to the most risk is outdated. The vast majority of web malware encounters happen on legitimate and trusted websites that you already visit.

Rise of Mobile Malware Disinformation

Android malware entered the mainstream consciousness in 2012 with explosive growth and the first documented botnet. Sensationalistic claims also came to a head, but mobile malware still makes up less than 0.5% of total web malware encounters.

Any Device, Many Clouds

Organizations are dealing with the outsized impact of securing any device across many clouds. Employees expect to use their devices to access applications and services from anywhere, and connectivity beyond the traditional desktop and server brings added complexity for security administrators.

Better Security Intelligence

The Annual Security Report provides a real-world perspective of the events that shape the threat landscape. This report, informed by Cisco's global security intelligence, can help you better defend your network.

Cisco Connected World Technology Report

The Annual Security Report includes findings from Chapter 2 of the Cisco Connected World Technology Report. In this study, you can read more about the security trade-offs that the world's next generation of workers - Generation Y - is making between privacy and the desire for social and personal online experiences.

Source and Further Reading:

A mysterious group of computer hackers has spent four years spying on the South Korea military, US security software maker McAfee said, citing evidence uncovered from malicious software samples.

"A mysterious group of computer hackers has spent four years spying on the South Korea military."

McAfee, a division of Intel, did not identify a sponsor for the attacks but said they were carried out by a hackers group known as the New Romanic Cyber Army Team. Seoul has blamed North Korea for some of the cyber-attacks although Pyongyang denies responsibility and says it too has been a victim.

Experts with Symantec, another security software maker, in June definitively linked the four-year string of attacks to a single group of hackers. The attacks hit government and corporate computers.

Sophisticated infrastructure

It said the hacking gang infected PCs with sophisticated software that automatically sought out documents of interest by scanning computers for military keywords in English and Korean.

"Once the software identified documents of interest, it encrypted those files then delivered them to the hackers' servers."

Once the software identified documents of interest, it encrypted those files then delivered them to the hackers’ servers, McAfee said.

McAfee named the attacks "Operation Troy", because the word Troy frequently appeared in the code of the malicious software. The New Romanic Cyber Army Team makes frequent use of Roman and classical terms in their code.

"It said the hacking gang infected PCs with sophisticated software that automatically sought out documents of interest by scanning computers for military keywords in English and Korean."

Source:
# Top Vulnerability List

These are currently the most significant vulnerabilities as reported by Symantec.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://example.com/image" alt="Medium" /></td>
<td>Oracle Java SE CVE-2013-1488 Remote Code Execution Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Microsoft Windows CVE-2012-1864 Local Privilege Escalation Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Oracle Java SE CVE-2013-2460 Remote Java Runtime Environment Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Oracle Java SE CVE-2013-2471 Buffer Overflow Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Oracle Java SE CVE-2013-2465 Memory Corruption Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Microsoft Internet Explorer CVE-2013-3893 Memory Corruption Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Intel CPU Hardware Local Privilege Escalation Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability</td>
</tr>
<tr>
<td><img src="https://example.com/image" alt="High" /></td>
<td>Oracle Java Runtime Environment CVE-2013-2423 Security Bypass Vulnerability</td>
</tr>
</tbody>
</table>

**Source:**
### Mozilla Foundation Security Advisory

**Risk:** Highly Critical  
**Products:** Firefox, Thunderbird  
**Reference:** http://secunia.com/advisories/54892/

### Security update available for Adobe Shockwave Player

**Priority:** 1  
**Severity:** Critical  

### Security Advisory for Adobe Reader and Acrobat

**Priority:** 1  
**Severity:** Critical  
**Reference:**  

### Security updates for Adobe Flash Player

**Priority:** 1  
**Severity:** Critical  

### Stable Channel Update for Chrome OS

**Description:** The Chrome team is excited to announce the promotion of Chrome 30 to the Stable channel for Windows, Mac, Linux and Chrome Frame. Chrome 30.0.1599.66 contains a number of fixes and improvements. This update includes 50 security fixes.  
**Reference:**  
## Apple Security Updates

<table>
<thead>
<tr>
<th>Product</th>
<th>Operating System Requirements</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 7.0.2</td>
<td>iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later</td>
<td>26 Sept 2013</td>
</tr>
<tr>
<td>Apple TV 6.0</td>
<td>Apple TV 2nd generation and later</td>
<td>19 Sept 2013</td>
</tr>
<tr>
<td>Xcode 5.0</td>
<td>OS X Mountain Lion v10.8.4 or later</td>
<td>18 Sept 2013</td>
</tr>
<tr>
<td>iOS 7</td>
<td>iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later</td>
<td>18 Sept 2013</td>
</tr>
<tr>
<td>iTunes 11.1</td>
<td>Windows 7, Vista, XP SP2 or later</td>
<td>18 Sept 2013</td>
</tr>
<tr>
<td>OS X Server v2.2.2</td>
<td>OS X Mountain Lion v10.8 or later</td>
<td>17 Sept 2013</td>
</tr>
<tr>
<td>Safari 5.1.10</td>
<td>Mac OS X v10.6.8</td>
<td>12 Sept 2013</td>
</tr>
<tr>
<td>OS X Mountain Lion v10.8.5 and Security Update 2013-004</td>
<td>Mac OS X v10.6.8, OS X Lion v10.7.5, OS X Mountain Lion v10.8 and v10.8.4</td>
<td>12 Sept 2013</td>
</tr>
</tbody>
</table>


## Adobe Digital Editions

**Description:** Adobe has released a security update for Adobe Digital Editions for Windows and Macintosh. This update addresses vulnerability in the software that could cause the application to crash and potentially allow an attacker to take control of the affected system.

**Priority:** 3

**Severity:** Critical


## Cisco

**Description:** Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

### Microsoft Security Summary for October 2013

**Description:**
The Microsoft Security Bulletin Summary for October 2013 describes multiple vulnerabilities in Microsoft software. Microsoft has released updates to address the vulnerabilities.

**Risk:**
- Remote Code Execution
- Information Disclosure

**Severity:**
Critical

**Products:**
- Microsoft Windows
- Internet Explorer
- Microsoft .NET Framework
- Microsoft Office
- Microsoft Server Software
- Microsoft Silverlight

**Reference:**

### Internet Explorer

**Description:**
Microsoft is investigating public reports of a vulnerability in all supported versions of Internet Explorer. Microsoft is aware of targeted attacks that attempt to exploit this vulnerability in Internet Explorer 8 and Internet Explorer 9.

On completion of this investigation, Microsoft will take the appropriate action to protect our customers, which may include providing a solution through our monthly security update release process, or an out-of-cycle security update, depending on customer needs.

**Reference:**
Global ICT solutions and services provider Dimension Data says that the number of devices on corporate IT networks carrying vulnerabilities has dropped from 75% in 2011 to 67% in 2012. While this is the lowest figure in two years, it highlights the on-going ‘lax approach’ to security on the part of network managers, says Dimension Data.

“On corporate networks, 67% of devices carry vulnerabilities.”

“There are certain vulnerabilities that have been around for many years which have not yet been fixed - despite vendors like Cisco Systems’ proactive approach to patch alerts and on-going software and system upgrades,” says Raoul Tecala, Dimension Data’s business development director for network integration.

“It can be a daunting and challenging task to eliminate all vulnerabilities from large and complicated environments. However, the disruption and effort required must be weighed against the potential impact and actions that must be taken. Although networks currently appear to have fewer vulnerabilities - the high percentage of devices carrying vulnerabilities will remain until the software is patched or upgraded to a newer, more secure version of code.”

Tecala advises organisations to focus their efforts on vulnerabilities that represent the largest threats.

“The closer a device is situated to the Internet, the higher the risk. Therefore, organisations must be vigilant and should implement a constant regime to evaluate, prioritise and patch network vulnerabilities.

“While IT networks currently seem to have fewer vulnerabilities - and many of these are difficult to eliminate completely - new vulnerabilities are identified each year, so it’s unwise to be complacent.” concludes Tecala.

Source and Further Reading:
Tuesday, April 8, 2014, could be a dark day for security administrators: That's the day Microsoft will end support for its Windows XP operating system. Since XP still runs on about one out of every four corporate PCs, enterprises may need security contingency plans unless they become more proactive and take steps to protect these systems, and soon.

Unveiled in October 2001, Windows XP has become a grey-beard among desktop operating systems. The OS's influence peaked at 76.1% market share and 400 million copies were sold as of January 2007.

In March 2008, Microsoft announced plans to phase out the OS. OEMs stopped bundling the Windows XP with their systems in June 2008, Microsoft ceased selling it in January 2009, and all support (including security patches) is slated to be dropped next April.

Yet, Windows XP still operates on 28% of corporate Windows computers, according to Ovum Research.

With Windows XP security updates ending in 2014, security vendor Sophos has warned of what it termed an upcoming XPocalypse if those numbers do not change. If XP is still running on so many corporate systems a year from now when regular software security patches stop coming, hackers will likely ramp up attacks on the OS beyond the frequent penetration seen today, putting corporate networks in greater danger.

“There's certainly the potential for a lot of havoc,” said Joshua Long, a security and networking specialist with Sophos and a contributor to its Naked Security blog.

“For instance, [a] new Internet-propagating worm that targets Windows X systems, or even just an increase in Internet Explorer 8 browser exploits, could open the doors wide for all manner of malware infections.”

So, how can a business protect itself from such problems? Microsoft, of course, would like companies to upgrade to newer versions of Windows, but doing so is not always in an enterprise's best interest.

"It can be difficult to build a sound business case for upgrading an operating system," noted Richard Edwards, principal analyst with U.K.-based Ovum.

“They can easily find business reasons to upgrade their applications, but the economics are not as clear with operating systems.”

“Hackers are now keenly focused on finding vulnerabilities with mobile systems,” Edwards said.

To protect corporate data from the threats unpatched XP machines present, it's clear that companies running XP will need to do something. Unfortunately, he said, many won't.

“We expect that XP will continue to be used in many enterprises throughout the rest of the decade,” Edwards concluded.

Source:
Top Malware List

These are currently the most prevalent malware as reported by Symantec.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Packed.Generic.443</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Trojan.Zbot!gen58</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>OSX.Hormesu</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Packed.Generic.442</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Backdoor.Prioxer.C!inf</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Backdoor.Prioxer.C</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Bloodhound.Mallnk.1</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Trojan.Ransomlock!g58</td>
<td>Trojan</td>
</tr>
<tr>
<td></td>
<td>Trojan.Ransomlock!g59</td>
<td>Trojan</td>
</tr>
</tbody>
</table>

Source:
Kaspersky Lab researchers today announced a new attack vector of NetTraveler (also known as “Travnet”, “Netfile” or “Red Star” APT), an advanced persistent threat that has already infected hundreds of high profile victims in more than 40 countries. Known targets of NetTraveler include Tibetan/Uyghur activists, oil industry companies, scientific research centres and institutes, universities, private companies, governments and governmental institutions, embassies and military contractors.

Immediately after the public exposure of the NetTraveler operations in June, 2013, the attackers shut down all known command and control systems and moved them to new servers in China, Hong Kong and Taiwan. They also continued the attacks unhindered, just like the current case shows.

Over the last few days, several spear-phishing e-mails were sent to multiple Uyghur activists. The Java exploit used to distribute this new variant of the Red Star APT was only recently patched in June 2013 and has a much higher success rate. The earlier attacks have used Office exploits (CVE-2012-0158) that was patched by Microsoft last April.

In addition to the use of spear-phishing e-mails, APT operators have adopted the watering hole technique (web redirections and drive-by downloads on rigged domains) to infect victims surfing the web. Over the last month, Kaspersky Lab intercepted and blocked a number of infection attempts from the “weststock[dot]org” domain, which is a known site linked to previous NetTraveler attacks. These redirections appear to come from other Uyghur-related websites that were compromised and infected by the NetTraveler attackers.

Kaspersky Lab’s Global Research and Analysis Team (GReAT) experts predict that other recent exploits could be integrated and used against the group’s targets and offer recommendations on how to stay safe from such attacks:

- Update Java to the most recent version or, if you don’t use Java, uninstall it.
- Update Microsoft Windows and Office to the latest versions.
- Update all other third party software, such as Adobe Reader.
- Use a secure browser such as Google Chrome, which has a faster development and patching cycle than Windows’ default Internet Explorer.
- Be wary of clicking on links and opening attachments from unknown persons.

“So far, we haven’t observed the use of zero-day vulnerabilities with the NetTraveler group. To defend against those, although patches don’t help, but technologies such as DefaultDeny and Automatic Exploit Prevention can be quite effective fighting advanced persistent threats”, - Costin Raiu, Director of Global Research & Analysis Team at Kaspersky Lab says.

Source: http://www.kaspersky.com/about/news/virus/2013/NetTraveler_is_back_with_new_tricks
Kaspersky's research uncovered that Red October, at the time of its discovery, had been active for at least five years, operating virtually undetected. Cyber-espionage attacks are not new, but they have become significantly more sophisticated. It's now often trivial for attackers to infiltrate organizations for months, if not years, without detection. But, by dissecting these advanced attacks, enterprises can learn important lessons.

**The Red October malware campaign uncovered**

Red October targeted several hundred victims since 2007, if not earlier. Its authors went after scientific research, diplomatic, government and supporting organizations across the globe, but mostly in Eastern Europe. Based on the text and names in the malware, Kaspersky Labs attributed the Red October modules to Russian-speaking developers and the exploit development to Chinese hackers.

The execution of the campaign proved to be similar to some other recent, high-profile attacks; it started with a phishing attack carrying a malicious attachment that, once executed, exploited Microsoft Office and Java vulnerabilities.

**Red October response: Examine existing, new controls**

In terms of lessons for enterprise security teams, Red October largely used attack methods that organizations should already be able to defend from, if they have security basics in place. Enterprises that haven't embraced the importance of anti-phishing, strong authentication, rapid patching and network monitoring will be successfully exploited by future Red October-like attacks. From there, additional supplemental defences are worth considering. Application whitelisting, for one, may have thwarted unauthorized executables on target systems. There's also a growing case to be made for emerging anomaly-detection products, like those from vendors such as FireEye and Damballa. Strong two-factor authentication, though not a new defence, could be used to prevent the attacks on the credentials.

Red October should be viewed as a signpost indicating where advanced attackers are going in terms of the comprehensive, multifunctional nature of their attacks and underscoring the importance of adjusting security programs to effectively defend against them. Like all other successful attacks, attackers will use the methods and ideas from the Red October campaign in future attacks, even if the attacks are publically known. Enterprises will need to plan for attacks that will rival the comprehensive nature of Red October in the coming years, as less sophisticated attackers adopt these new tactics. Enterprises should prioritize efforts to reassess their environments and determine where controls can be improved or new ones implemented to prevent similar attacks.

Source:

Combating malware is a constant struggle, with new forms being developed daily. The best way for enterprises to defend themselves is to be aware of the new malware threats, implement application policies, and devise antimalware techniques. This expert E-Guide uncovers the best tactics for creating a successful antimalware protection strategy.

While IT continues to fight increasingly clever attacks against on-site enterprise infrastructure, new malware is taking aim at lower-hanging fruit: under-secured smartphones, mobile applications, social media, and other cloud services. As workers make more extensive use of such perimeter-less platforms, they create rich targets that require new antimalware protection strategies to mitigate these multifaceted new malware threats.

Enterprises can defend themselves by understanding these new malware vectors, enforcing application policies, implementing new device resident and cloud-based antimalware techniques, and leveraging other security tools.

Following the money
Far more than fame or hacktivism, the malware industry is driven by financial gain and drawn to low-cost, high-profit attacks. This has been repeatedly proven, as malware migrated from floppy to USB drives, email to Web, browser to PDF, abandoning old haunts to seek out more vulnerable monocultures.

Social media security risks
For IT groups scrambling to stop malware on so many different fronts, deciding which threats to tackle can be a challenge. The best place to begin is by understanding emerging malware: targeted platforms, exploited vulnerabilities, and jeopardized business assets.

“Recently, the biggest threats have not attacked computers -- they’ve attacked people.”

To date, social media malware has gotten the biggest bang by aiming at Facebook, Twitter, and YouTube. For example, Twitter’s brevity, anonymity, and real-time communication have fostered many hacks since 2007 – some involving account compromise, others malware dissemination. The two are intertwined, as legitimate and fraudulent top-followed accounts are used to phish thousands of victims. Shortened links, trend tags, and direct messaging further increase the odds of following tweets to malware.
Workforce and malware mobility

In fact, consumer mobile network attach rates are skyrocketing, driven largely by bring-your-own devices. According McAfee Senior Architect Igor Muttik, these unmanaged smartphones and tablets pose real enterprise risk.

“Mobile devices are no longer just phones; they are now full computing devices. For example, they can record audio and video for blackmail or industrial espionage. —If somebody brings their device into the office, IT has no idea what’s on it. A blanket ban on personal devices isn’t going to succeed, so measurement of security is essential before allowing devices in or rejecting them.”

Rolling out new antimalware protection

Additional strategies likely are needed to mitigate business-affecting malware delivered and executed outside corporate networks. New device-resident and in-the-cloud antimalware approaches can complement existing defences.

Specifically, MDM can not only mandate passwords and invoke remote wipe; it can also remotely install (or direct users to) mobile antimalware apps. Such scanners are readily available for Android, but not effective on iPhones or iPads due to OS restrictions.

Stopping malware inside the corporate network

Even experts with vested interest in new antimalware approaches recommend leveraging other types of security tools to battle malware, such as next-generation firewalls, secure Web gateways, data loss prevention and network behaviour analysis. This strategy may not stop external infection, but it can reduce business impact, especially if platforms are reputation-aware.

Malware is an on-going battle; we can be certain that attackers will continue to develop new malicious code and target new technology trends. But by raising awareness of new vulnerabilities and threats, and mitigating them through a multi-pronged antimalware strategy, enterprises arm themselves with a fighting chance against evolving threats.

“Leveraging other types of security tools to battle malware, such as next-generation firewalls, secure Web gateways, data loss prevention and network behavior analysis.”

Source and Further Reading:
Research shows some startling figures, including:

- 10% of laptops are lost over the lifetime of the device
- Devices are most often stolen at the office (52%) or at a conference (24%)
- Laptops are most often lost or stolen offsite (47%) or in transit (29%)
- 70 million smartphones are lost each year – only 7% are recovered
- 50% of all mobile device users keep passwords, personal information and credit card info on their device
- 36% of tablets contain confidential work-related information

"If a well-implemented security policy can reduce laptop theft by 85%, there’s more reason than ever to invest the time in reviewing your practices."

Source:

Recommended practices in securing mobile devices:
- Implement a mobile security policy
- Invest in physical security
- Never leave devices logged into networks, email or websites
- Encrypt all data and secure networks
- Authenticate users and always know who has access
Airports continue to be a top location for device theft, which isn’t surprising. Devices are often carried by people when traveling for business and pleasure. The owners are usually in a rush to make their flight and are not familiar with their surroundings, providing thieves with the perfect opportunity to snap up an unattended device.

Source:
The following steps are a good start in preventing information or system compromise:

**Store only what you absolutely need.** This is my first rule of data leakage protection. Why carry around customer spread sheets, financial data, or plans for a new product/service if you don’t need them while out of the office? Absent Information can’t be compromised.

**Protect data passing over public wired or wireless networks.** The best way to prevent casual or directed packet snooping on public networks is packet or session encryption, even if encryption is limited to only traffic between the end-user device and a traffic encryption service provider on the Internet. For ultimate protection, use only SSL connections to check e-mail or access company information. Two examples are MegaProxy (fee-based) and AnchorFree (free).

**Configure devices to block external snooping.** The first step in establishing a security perimeter around a device is configuration of a firewall. Personal firewalls are free on laptops running Windows XP or Vista. These solutions provide minimal protection against intruder compromise of your mobile system. More complete protection is available in security suites, like those from AVG, McAfee, or Symantec. Firewalls are also available for many handheld devices, protecting contact lists, e-mail, and other sensitive information commonly found on PDAs and smartphones. The second step is configuring Bluetooth, on laptops and handhelds, to block all unauthorized access. Bluetooth threats and secure configuration information is found in Secure your Bluetooth wireless networks and protect your data. No laptop should be unnecessarily exposed because it lacks anti-malware protection.

**Encrypt sensitive information on the device.** I know this is like beating the proverbial dead horse for many, but laptop theft reports make it clear that many users and organizations haven’t yet gotten the message. And laptop encryption doesn’t have to drain your budget. Solutions like TrueCrypt provide effective, free file and full-disk encryption. If you need a more centralized approach to key management, lost data destruction, or data recovery, online services like Beachhead or more traditional systems like PGP can help.

**Backup critical information.** All business critical information should be copied to an alternate location. Even mobile users, who might not connect to the company network every day, can be protected against data loss with online solutions like Symantec’s backup.com or with Amazon.com’s S3 service, supported with client software like Jungle Disk.

And of course, practice standard system hardening practices—patching, shutting down all unneeded services, etc. In addition to following Microsoft’s best practices, consider implementing some or all NIST (National Institute of Standards and Technology) recommendations and baseline template settings.

---

**Source:**

http://www.techrepublic.com/blog/it-security/five-steps-to-protect-mobile-devices-anywhere-anytime/
Does your laptop hold your personal data? What would you do if it were stolen? Consider these statistics:

- One laptop is stolen every 53 seconds (Gartner)
- 97% of stolen laptops and computers are never recovered
- 65-70% of lost laptops are never reclaimed
- 53% of business travellers carry sensitive corporate information in their laptops

When your laptop gets stolen, you lose a lot more than your computer and the cost of the replacement; that is why it makes sense to take these simple steps to protect it.

- Don’t let your computer out of your sight, even for a moment. Wi-Fi hotspots like coffee shops can be distracting and are prime hangouts for laptop thieves. Don’t leave it on a table to get a refill, and don’t put it on the floor behind your chair.
- If you are out and about with your laptop, take it with you rather than leave it in the car. If you must leave it in the car, don’t leave it on the seat. Hide it under the seat or in the trunk, or you could end up with a stolen laptop and a broken car window. This is just common sense; don’t offer thieves a reason to break into your car.
- If you’re traveling with it, don’t leave it in your hotel room unless you’ve secured it with a laptop cable lock. If you don’t have a laptop cable lock, take it with you or ask hotel management to lock it up. Microsoft offers some other tips for traveling with your laptop. (Below)
- Write down your laptop’s serial number and store it safely. It will help the police recover your laptop if it is stolen.
- Get a laptop tracking device installed.

Finally, don’t forget to back up your files and keep a copy of the backup in a separate location away from your laptop — not in your laptop bag because it may get stolen along with the laptop itself. Although this won’t prevent your laptop from being stolen, it will take a lot of the sting out of losing it.

Many of these are common-sense approaches to preventing theft.
As technologies advance, mobile phones, tablets and notebook computers are becoming more and more commonplace. Mobile devices are capable of storing and processing large amounts of information without having a fixed physical location.

“A stolen or lost mobile device with unprotected storage allows an attacker to access the data on it. If the device is infected with malware, it may lead to hidden use of premium services, or leaking sensitive information. Here are some general tips for maintaining the security of your mobile device.

When configuring your mobile device

- Enable a power-on password or other device password management tool if available.
- Configure the mobile device in such a way that it locks automatically after some inactive time.
- Install mobile security software, such as anti-virus software and firewall on mobile device if available.
- Apply the latest patches and fixes for your mobile operating system and related backup/synchronisation software. Upgrade the software to its latest version where applicable.
- Scrutinise thoroughly all permission requests, for example those involving privileged access, when installing applications/services.
- Use encryption to lock sensitive data stored on the mobile device and removable media, if available.
- Set up a remote data wiping feature if available.
- Turn off wireless connections such as Wi-Fi, Bluetooth and/or infrared connectivity when not in use.
- Turn off location services setting in your mobile device if it is not necessary to run location-based application.
- Do not jailbreak the mobile device (to override usage and/or access limitations).

When using your mobile device

- Do not leave a mobile device unattended, even for a moment.
- Do not process sensitive data in the mobile device unless with encryption feature on or secure end-to-end connection.
- Do not open or follow links in SMS/MMS or email from misleading URL, suspicious or untrusted sources.
- Do not download or accept programs and content from unknown or untrusted sources.
- Be cautious when connecting to publicly available Wi-Fi hotspots, and avoid access sensitive data unless with adequate security protection.
When backing data in your mobile device
- Turn on the encryption option in the backup/synchronisation software for storing the data in encrypted mode if available.
- Make sure the backup copies are encrypted no matter if it is stored on a desktop PC or on removable media.

When disposing your mobile device
- Completely clear all data and settings on your mobile device before disposal.

At ALL times
- Keep your mobile devices in a secure place, especially when not in use.
- Stay alert on security vulnerability on mobile devices, and apply the latest patches and fixes when available.
- Do not install illegal or unauthorised software on the mobile device.
- Do not allow wireless connections from unknown or untrusted sources on your device.

“Keep your mobile devices in a secure place, especially when not in use.”

Smishing is a combination of the terms "SMS" and "phishing." It is similar to phishing, but refers to fraudulent messages sent over SMS (text messaging) rather than email.

“Smishing is a combination of the terms "SMS" and "phishing."”

The goal of smishing is to capture people’s personal information.

Smishing has become increasingly common now that smartphones are widely used. Many smartphones allow you to simply click on a link in a text message to view the website in your phone’s browser. This makes text messages an effective “bait” for luring unsuspecting users to fraudulent websites. Therefore, just like when you receive email spam, is best to not visit websites mentioned in text messages from unknown sources.

Source:

Source:
http://www.techterms.com/definition/smishing
**Topic of Interest**

**Assistance with Lost or Stolen Devices**

**Android Lost**

Find the location of your phone on a map. With AndroidLost you can find your phone with GPS precision. Even if the phone is indoors you will get a nearby location by network accuracy.

You can lock and unlock the phone from the web. If you forget your pincode you can simply overwrite it or remove it from the web.

Don't want your personal messages in the hands of anyone else? With AndroidLost you may wipe the entire phone so all SMS'es, contact and Google setup is removed.


**Blackberry Protect**

You've lost your smartphone. Why wonder who has access to your information? Simply log in to the BlackBerry Protect website and lock your device.

Pretty sure you’re not going to see it again? You can delete the information on your smartphone from the BlackBerry Protect website.

Your contacts, text messages, calendar and bookmarks can be backed up wirelessly. It’s done automatically, and as often as you choose.


**Find my iPhone**

If you lose your iOS device or think it might be stolen, these steps may help you locate it and protect your personal data.

If you enabled Find My iPhone on your missing device

- Attempt to locate your device using Find My iPhone at iCloud.com/find, or using the free Find My iPhone app.
- Put the device in Lost Mode.
- If you want to delete all of your personal information from your missing device, you can erase it remotely.

If you did not enable Find My iPhone on your missing device

- Change your iCloud password to ensure that no one else can use your device to delete or make changes to your iCloud data.

http://support.apple.com/kb/HT5668
Following a recent spate of SIM swap banking fraud, the South African Banking Risk Information Centre (Sabric) – together with mobile operators and law enforcement entities – is working to combat cybercrime and spread awareness.

Sabric has urged SA’s consumers to adopt stricter personal IT security measures and, as part of its education campaign on SIM swap fraud and the rising threat of phishing, the body has issued the following tips to avoid falling victim to crime online:

- Never respond to e-mails that appear to be from your bank and request personal details. Remember no bank will ever ask you to confirm or update account details via e-mail, SMS or telephone.
- Never follow a link on an e-mail to access your bank’s Web page. Always access the page by physically typing the name of the Web address that you were given when you signed up for Internet banking in your browser, and confirm you are on a secure site by looking for the “lock” icon on the browser before logging on.
- Never provide your online ID, password or PIN to anyone and never write them down or share them – not even with a bank official.
- Do not save your Internet banking password on your desktop.
- Do not make passwords too personal. Preferably create passwords that have letters, numbers and symbols in them that cannot be attributed to you.
- Do not leave your computer unattended after entering your Internet banking password.
- Always log off or sign off at the end of a session.
- Avoid doing Internet banking in public areas such as Internet cafés, or on any computer that can be accessed by people you do not know.
- Change your PIN and passwords frequently.
- Place sensible transaction limits on your accounts.
- Ensure you have the latest anti-virus software applications loaded on your computer, and make sure you download all security patches for your operating system in a timely fashion.
- Only provide your credit card details to reputable companies.
- Do not open e-mail from unknown sources – delete them immediately, even if the title and sender details appear to be related to your bank.

“Sabric warns cyber crime in on the rise – but there are ways to mitigate your risks.”
Avoid becoming a SIM swap fraud victim...

Avoid SIM swap fraud

The first line of defence against SIM swap fraud specifically, says Sabric, is to protect personal and cellphone account information from third parties and Web sites. This information, which mobile operators will ask for during the SIM swap process, includes cellphone contract type, debit order dates, identity number, addresses and transaction behaviour. Sabric suggests:

1. Be vigilant and always aware of your mobile phone’s network connectivity status. If you realise you are not receiving any calls or SMS notifications, something may be wrong and you should make enquiries to be sure you have not fallen victim to this scam.

2. Some mobile operators send customers an SMS to alert them of a SIM swap instruction and customers should contact their operator if the request is fraudulent.

3. Do not switch off your mobile phone in the event you are receiving numerous annoying calls, rather not answer the calls. This could be a ploy to prevent you from noticing your connectivity has been tampered with.

4. Have your mobile phone services provider’s numbers written down somewhere close by. This way you can phone to check whether anything suspicious has taken place.

5. Register for SMS notifications when there is any activity on your bank account so that you can be alerted to any attempt to move funds from your account.

6. If already registered for SMS notifications, keep your mobile phone with you and on at all times so that you can respond to any suspicious activity immediately.

7. SIM swap fraud almost always works hand-in-hand with phishing/smishing, so the same protection mechanisms should also apply (do not click on links from e-mails, SMSes, etc, purporting to be from your bank and never enter your log-on information).

8. Make a habit of checking bank statements and online banking transaction history regularly. In this way, you will able to timeously identify any unauthorised transactions.

Source:
http://www.itweb.co.za/index.php?option=com_content&view=article&id=64377&A
Developing a remote management strategy that dictates what tools the network security staff can use in order to access their equipment is important. Giving staff the flexibility to manage equipment remotely is common, but doing so shouldn't create holes in the company's security posture. Here are a few key factors to consider to help determine how to implement a remote management program:

- **Determine how they'll get access.** Not everyone should have access remotely. First, clearly defined and documented policy and procedures must be in place to approve authorization for someone to manage the network remotely. This isn't something you want to take lightly: Each individual's job role and responsibilities should be taken into account, as well as his or her personal history with the company. Such checks and balances must in place to ensure that those who gain remote access to key network and systems infrastructure don't abuse that access.

- **Determine what they'll have access to.** Determine what privileges a particular admin is capable of accessing after they've remotely entered into the network. There are valid reasons that you would want to segment what an administrator is capable of accessing remotely. For example, you might want to ensure that the administrators of systems that generate logs do not have access to a centralized log management console that would allow them to tamper with those logs. Decisions for provisioning remote access should be made using the same least-privilege approach as local access.

- **Determine when they'll need access.** Are they going to need access to your company's network all the time? Are they administrators or consultants? Do you want these users in the network at any given time, and from any location? Make sure you have the proper restrictions in place when and where needed.

Once these questions are answered, pick a method and tool for them to access the network. When searching for a remote access tool to use, first determine if the tool or application has the ability to encrypt remote traffic, use multiform authentication and has the ability to log and audit data. There are many tools and ways to get into the network, but security is the main concern. If a tool can't encrypt, log or have multiform authentication, it shouldn't be used. Use these three features as a baseline when searching for remote management tools.

“First determine if the tool or application has the ability to encrypt remote traffic, use multiform authentication and has the ability to log and audit data.”

Source:
The goal of the Critical Controls is to protect critical assets, infrastructure, and information by strengthening your organization's defensive posture through continuous, automated protection and monitoring of your sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs.

The strength of the Critical Controls is that they reflect the combined knowledge of actual attacks and effective defences of experts in the many organizations that have exclusive and deep knowledge about current threats.

The five critical tenets of an effective cyber defence system as reflected in the Critical Controls are:

- **Offense informs defence**: Use knowledge of actual attacks that have compromised systems to provide the foundation to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks.

- **Prioritization**: Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in your computing environment.

- **Metrics**: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

- **Continuous monitoring**: Carry out continuous monitoring to test and validate the effectiveness of current security measures.

- **Automation**: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the controls and related metrics.

While there is no such thing as absolute protection, proper implementation of the security controls identified in this document will ensure that an organization is protecting itself against the most significant attacks.

Source:
SANS Top 20 List of Controls...

Critical Control 1: Inventory of Authorized and Unauthorized Devices
Critical Control 2: Inventory of Authorized and Unauthorized Software
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
Critical Control 4: Continuous Vulnerability Assessment and Remediation
Critical Control 5: Malware Defences
Critical Control 6: Application Software Security
Critical Control 7: Wireless Device Control
Critical Control 8: Data Recovery Capability
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
Critical Control 12: Controlled Use of Administrative Privileges
Critical Control 13: Boundary Defence
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs
Critical Control 15: Controlled Access Based on the Need to Know
Critical Control 16: Account Monitoring and Control
Critical Control 17: Data Loss Prevention
Critical Control 18: Incident Response Capability
Critical Control 19: Secure Network Engineering
Critical Control 20: Penetration Tests and Red Team Exercises

“AInventory of Authorized and Unauthorized Devices and Software.”

Source:
http://www.sans.org/critical-security-controls/control.php?id=18
As cyber-crimes become increasingly advanced, pervasive, and costly, organizations are pondering how secure their enterprise really is. While not an easy question to answer, the Security Maturity model from HP offers insight on steps you can take to mitigate risks and ways to improve agility.

Inside, learn more about the Security Maturity model and states of enterprise readiness to get help determining where on the security curve you are – and where you need to be.

In addition, view five security questions every CIO should be able to answer and learn how you can take security intelligence to the next level.

How Secure Are You?

Cyber crime. The very word sets many CIO’s hearts racing. Although far from a new threat, cyber crime is getting increasingly sophisticated, often nipping at the heels or surpassing the security of enterprises. Security tools and programs are constantly evolving to meet the new challenges, and security planning is no longer just an annual event. As attack methods change, so too must defence strategies if they are to stay ahead of the curve.

As cyber crime becomes increasingly advanced, it is also becoming pervasive and costly. The 2012 Cost of Cyber Crime survey conducted by the Pokémon Institute and sponsored by HP examined 56 companies across all industry verticals to get a picture of the impact and costs of cyber crime. Companies across the survey base experienced an average of 102 successful attacks a week, an increase of nearly 42 percent over the 72 attacks per week experienced in 2011. Complicating matters was the fact that the attacks were stealthier than in the past, which led to longer remediation times. The study found it took an average of 24 days to contain a cyber attack, up from 18 days in 2011.

The Security Maturity model, shown in Figure 1, asks enterprises to look at what steps they are taking to mitigate risk factors while improving their agility as they prevent, detect, and remediate attacks. Where an enterprise is on the continuum determines the maturity of its IT security management. While not every enterprise will need predictive capabilities, most will need to go beyond basic defensive protections. And all enterprises can benefit from a more integrated approach. An offensive strategy can protect against more sophisticated threats and even against undetected breaches that may have occurred long ago.
States of Enterprise Readiness

Basic Tools: As a basic defence, perimeter protection, such as intrusion detection, can identify and report a potential security attack. HP was the first to go a step further, offering intrusion prevention, which not only identifies suspicious network activity but also blocks malicious executables and files, more quickly stopping potential damage.

Layered Tools: A layered approach is typically called “defence in depth.” It uses multiple tools and policies to safeguard various attack vectors including system, network, and application levels as well as data transmissions. A layered approach enables faster reaction against a broader set of threats.

While layered tools provide a tremendous amount of protection, for enterprises focused on compliance requirements, they are a bit like looking in your rear-view mirror. Compliance alone tends to focus on the lowest common denominator—what can the majority of enterprises subject to the controls feasibly do? If compliance were a high bar, a majority would fail regulatory audits. Cyber attackers are infinitely more advanced than average security controls. For this reason, most organizations will need to look beyond point products offered by individual security tools.

Integrated Tools: The more security-mature enterprise looks to correlation, situational context, and integration to provide the best insight and protection. At the same time, common management may afford efficiencies for security operations.

“Where Are You on the Curve?”

Proactive Tools: Proactive tools are designed to catch potential threats with the most business risk. Examples of proactive approaches include application vulnerability assessments, incorporation of threat intelligence, and IT governance, risk and compliance (IT GRC) management.

Predictive Tools: Predictive tools use advanced analytics to identify potential attacks via patterns in external data. This approach protects against unimagined, and thus unanticipated, threats—before they ever appear as a security event in traditional security systems. With these tools, enterprises take an offensive strategy.

Where Are You on the Curve?

How secure are you? How much security is enough? Although it is important to meet compliance requirements and secure the perimeter, remember that threats are constantly evolving. As the adversaries become more sophisticated, so must your capabilities.

And before deciding where on the curve you need to be, it is important to determine where you are. In addition to the tools mentioned in this article, what processes do you have in place, and how mature is your overall security and compliance program?
Profitability and growth are two signs that a business is successful. To achieve these, companies must be well managed, agile, and innovative. But they also need to be secure, and that means protecting their intellectual property, business services and data, and the privacy of their customers.

Enterprise security is becoming increasingly complex, and the CIO’s job is becoming harder for two principal reasons. First, it’s no longer enough to secure the business perimeter and keep hackers off the corporate network. That’s because new IT trends like cloud computing and mobility mean there is no clearly defined perimeter to secure.

Second, the security threats enterprises face are growing — in frequency, in type, and in complexity. Organized crime gangs, hacktivist groups, and even foreign government-backed experts pose a far greater threat today than the opportunistic amateur hackers of the past. There is also the problem of identifying threats that originate inside the organization — these include malicious employees or contractors and industrial spies along with well-meaning employees who inadvertently compromise security.

The bottom line is that these threats introduce security risks, and since they can’t be eliminated completely, they must be managed, just like financial or physical asset risks. Investment in enterprise security is, in a sense, a form of insurance. It can help reduce the likelihood of a security breach, minimize the impact if one does occur, and allow for faster recovery. Like any insurance, it comes at a price, but the alternative is a greater risk of incurring costs or damaging brand reputation.

To properly manage such risks, CIOs must have answers for five critical questions.

**Question 1:** How are we ensuring compliance with privacy laws and other regulations here and abroad?

Taking steps to keep confidential customer data secure is considered so important that privacy laws set out legal requirements with which enterprises are required to comply.

**Question 2:** How are we protecting ourselves in a world dominated by mobile devices and free Wi-Fi?

The most effective way for companies to protect themselves against device risks is to implement a mobile device management system. To bring mobile devices under enterprise control by enforcing security policies, such as requiring the contents be encrypted and requiring a long password to unlock the device. They can also lock or remotely wipe lost or stolen devices. Another layer would be identity management, which ensures only authorized users have access to the data.

Mobile devices also introduce “application risk”: Malicious apps on a mobile device may access sensitive data on the device and send it to third parties. Applications designed to provide customers or staff access to corporate systems, but that have weaknesses like poorly implemented cryptography or poor authentication may be exploited by hackers to compromise corporate security.
Question 3: How do we ensure cloud applications being used are secure?

It is the customer’s responsibility to ensure that the cloud provider’s security measures and claims are effective and credible. That could involve examining its policies and procedures, ensuring relevant certifications have been obtained, or even assessing proprietary source code.

Customers are also frequently responsible for data encryption to ensure the security of any data stored by the cloud service provider. This can be achieved by controlling and managing encryption keys and carrying out encryption at a gateway to the cloud provider.

The most effective way to deal with the risks of cloud applications is to run them in a private cloud in a data center over which an organization has complete control. This is not always feasible. Enterprises thinking of running applications in external clouds should first consider a thorough analysis of the cloud provider’s security measures.

Question 4: How are we defending ourselves from internal threats?

Internal threats include malicious employees or ex-employees — often IT staff — who use their privileged position in an organization to access, destroy or steal data, or cause damage. But loyal employees can unwittingly pose an internal threat to an organization as well. They might, for example, provide passwords or other authentication credentials to a hacker, perhaps through a social engineering attack or phishing scam. They may also inadvertently download a malicious application that provides a hacker with access to computer systems, or take data home on a USB stick, where it is outside the protection of any corporate security systems.

Question 5: How do we know if our security investments protect our most critical business functions?

No security infrastructure can provide 100 percent security, and that’s why investments in security are about risk management. Hence, organizations must invest in areas where the risks to the business are the most significant, bringing them down to acceptable levels. Like any investment, security spending needs to be evaluated according to the likely return (in terms of reduced risk) that it will produce, and budgets allocated accordingly.

Understanding composite risk to your most important business assets and functions is key. Composite risk is made up of:

- **Real-time risks** — What risks or threats have actually manifested on my network?
- **Vulnerability risks** — How do I aggregate risk scores as I roll up my IT asset hierarchy to business functions?
- **Compliance risks** — How does configuration and policy drift factor add to risk?
- **Intrinsic risks** — How mature are the people and processes around my controls?
- **Extrinsic risks** — How do external factors (like earthquakes) factor into overall risk?

Enterprises should look holistically at the business. They should know which business functions are most important and which IT assets support them. Then, they must continuously assess the composite, real-time risk of those areas to determine how security spending should be allocated and risks mitigated.

Conclusion

The threats that enterprises face are growing, so the security measures implemented must evolve to mitigate new risks as they emerge. It’s a continuous process, and if you fall behind, the consequences can be very serious indeed.

A security assessment carried out by independent experts is the first step in this on-going relationship. Much like seeking out a third party to assess your insurance coverage, assessing your security and risk management program provides a necessary level of protection — particularly if you are unsure of answers to these questions.

Source and Further Reading:

http://searchsecurity.bitpipe.com/data/loadAsset.action?resId=1371061792_872
ECS-CSIRT is the government Computer Security Incident Response Team (CSIRT) within the State Security Agency (SSA).

The ECS-CSIRT uses the following address for all email communications - ecs-csirt@e-comsec.com

The ECS-CSIRT website - www.ssa.gov.za/CSIRT.aspx

Please also feel free to forward this newsletter to colleagues that may be interested in this newsletter.

Please take the time to reply to us with any suggestions you may have, so that we can provide a better service to you.