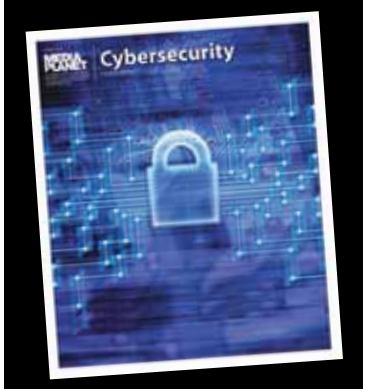
MARCH 2010

MEDIA PLANET

Cybersecurity

YOUR GUIDE TO PROTECTING YOURSELF ONLINE



CONTENTS

MEDIA PLANET

CYBERSECURITY

Publisher: Geraldine Delacuesta
geraldine.delacuesta@mediaplanet.com

Contributor: David Duffy

Designer: Carrie Reagh
carrie.reagh@mediaplanet.com

Photos: ©iStockphoto.com

Printer: The Washington Post

For more information about supplements in the daily press, please contact
Kayvan Salmanpour, 1 646 922 1400
kayvan.salmanpour@mediaplanet.com

This section was written by Mediaplanet and did not involve The Washington Post News or Editorial Departments.

www.mediaplanet.com

The Changing Landscape Of Cybersecurity

BY: KEVIN RICHARDS

If you look up the term "cybersecurity," you'll find the definition "…measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack."

Kevin Richards

ISSA® Information Systems Security Association

"This definition has now become outdated. The future of cybersecurity transcends far beyond protecting computers, and is focused squarely on protecting companies, customers, and families. Technology has been integrated into seemingly every aspect of our day-to-day lives—the way we communicate, the way we work, and the way we interact with the world around us. In many cases, it is indistinguishable when the human element leaves a process and technology picks up. With all of the technological advances, though, new challenges have arisen. Whether through error or malicious exploitation, technology, and the way we use technology, has uncovered flaws—sometimes with severe repercussions. These errors have caused devastating results—millions of personal identities have been lost or stolen, the power grid has come under attack, and, to the extreme, it has cost people's lives. In response to the challenges, the future of cybersecurity cannot revolve around a computer; it must evolve to protecting the people and companies impacted by the exposures in the technology.

A major challenge of cybersecurity is the continually changing landscape of what we are trying to protect. Our information is seemingly everywhere—on laptops, smart phones, USB jump drives, "in the cloud"—and it's ever on the move. Add to the equation that the corporate definable and protectable logical perimeter has all but eroded, and the result is seemingly an infinite amount of critical information being stored and shared on a growing and moving array of computing environments.

The other side of the equation is a motivated, aggressive and organized attacker community. Data is big business, and these groups have hired some serious talent. Through extensive botnet networks and bleeding-edge "zero-day" attack strategies, there is a new landscape of information warfare. These exploits span multiple vectors—phishing, application vulnerabilities, social engineering—and thrive in an environment where a security strategy is defined by legacy platforms and IT general controls. The future of cybersecurity needs to consider a data centric model rather than a perimeter based strategy to defend against the next generation of attacker.

Whether through chat, texting, or social networking, the way we communicate and collaborate has changed dramatically as well—140-character bursts have become common interaction. The future of cybersecurity needs to embrace these new mediums, teaching users appropriate ways to interact in these venues, while still achieving corporate risk management goals. This education needs to extend well beyond the corporate landscape as well to reach our children, helping to defend against cyberbullying and cyberhazing.

As we move into this new decade, the definition, and practice, of cybersecurity must extend beyond the protection of a computer to be considered successful. Anything less will leave us well short of protecting the things we hold most dear.

Kevin Richards, CISSP, is the President of the ISSA International (www.issa.org) and is the Director of Risk and Security Services for Neohapsis (www.neohapsis.com).

> "Whether through chat, texting, or social networking, the way we communicate and collaborate has changed dramatically as well—140-character bursts have become common interaction."

A VERY SPECIAL THANKS TO...

Family Online Safety Institute

StaySafeOnline.org National Cyber Security Alliance

wired SAFETY

VISA CURRENCY OF progress

NETWITNESS

NEOHAPSIS

Everyone is a risk manager.

Every member of your organization makes risk management decisions on a daily basis. Our governance, risk, and compliance solutions help people understand those risks to make smarter business decisions.

Neohapsis – The Power of Security and GRC

NEOHAPSIS

www.neohapsis.com

Phishing, Pharming and Bots: A Short Guide to Malware

"Lions and tigers and bears—oh my!" Dorothy and her companions chant to ward off their fears in The Wizard of Oz. Internet users might try, "Trojans and rootkits and bots!"

Dorothy's fears were mostly imaginary, but the threats online are all too real—and growing. Malware, malicious software, has become a leading online scourge, evolving in a short decade from so-called worms and viruses conceived principally to vandalize, to sophisticated spyware and crimeware designed to steal—money, information and identities.

Kaspersky Lab, a security firm specializing in combating malware, collected nearly 34 million malicious programs by year-end of 2009—including some 15 million each in 2008 and 2009. In its Security Bulletin 2009, the company says "programs became significantly more complex in 2009 and targeted new platforms such as mobile operating systems."

Symantec, a leading online security company, says on its web site, "The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers is now ruled by a new breed of cybercriminals."

Malware has long been delivered hiding inside trojans—innocent-appearing emails or software. In an irony only a cyber criminal could appreciate, 2009 saw big increases in rogue antivirus software used as malware delivery vehicles, according to Kaspersky. Once launched, rootkit programs keep the invasive software concealed.

Phishing is a favorite technique—emails that use fear or enticement to encourage recipients to click on a link or visit a web site that steals or corrupts their data. Pharming programs are even more insidious—they redirect unsuspecting users to fraudulent web sites, even if the user types in a correct URL. The bad guy's goal is installation of spyware on your computer or network—programs that log your keystrokes, steal usernames and passwords, or enable access of your bank or credit card accounts.

Yet another set of applications can turn your computer into a zombie or bot—essentially a dedicated slave used by cyber criminals to launch anonymous spam assaults or distributed denial of service (DDoS) attacks against the online presence of a company, organization or entire nation. Estonia, Georgia, South Korea and the United States have been targets of DDoS attacks in recent years.

> "Don't click on unfamiliar links, even if sent by someone you know."

The complexity and sophistication of cyber crime grows quickly, but—fortunately—some of the best defenses remain straightforward and based in common sense. Don't open (and do delete) unsolicited emails. Don't click on unfamiliar links, even if sent by someone you know (their computer could be being used as a bot). Don't download software from a strange web site (no matter how enticing the deal)! Scan all emails and files with a recognized antivirus security program. Keep all security patches up-to-date.

Online threats are real. You need more than a catchy chant to protect yourself.

Digital Citizenry

BY: MICHAEL KAISER, EXECUTIVE DIRECTOR, NATIONAL CYBERSECURITY ALLIANCE

Cybersecurity is a hot topic these days. Malware, botnets, hackers, cyber-terrorism, phishing, spear phishing, cyber-espionage, identity theft, etc. are all talked about by industry insiders as serious threats we need to protect ourselves and the critical infrastructure from.

But what does all of this mean for the average citizen? The everyday computer user who isn't an IT professional or doesn't have a degree in computer science but is simply using technology in the workplace, at school, or at home?

The Internet can be viewed as an eco-system, made up of networks, computers and people that are interconnected. Anytime a threat emerges in one part of the Internet it has the potential to impact the rest of the digital ecosystem. We value the Internet for how it enhances our lives and, similar to the environment, we need to work together to protect the digital assets we all share from abuse and misuse. Each of us has a responsibility to protect cyberspace by making sure the computers and networks we use are secure and that we employ good judgment online. What you can do to be a digital citizen:

1. Use security software tools (anti-virus, anti-malware, firewall) as your first line of defense.
2. Keep all of your software, including your web browsers and operating systems, up-to-date.
3. Back up important files.
4. Use strong passwords or authentication technology to help protect your personal information.
5. Secure your wireless and mobile devices.
6. Learn what to do if something goes wrong.
7. Use good judgment online. Ask yourself the **3 W's: W**ho am I communicating with? **W**hat is the value of the information being shared? **W**hy do I need to share it?
8. Teach your children how to protect themselves and use critical thinking skills to make good judgment about what they do online.
9. Learn more: visit www.staysafeonline.org

Cyberthreats:

Moving The Federal Fight Forward

Howard Schmidt, the recently appointed White House cybersecurity director, takes issue with the term cyberwarfare.

"A cyberwar is just something that we can't define," he told security education web site govinfosecurity.com. Amit Yoran, former director of US-CERT (Computer Emergency Readiness Team) and the National Cybersecurity Division of the Department of Homeland Security, says he tends to agree. "It's a sensational term that conjures threat images and legal and policy frames of reference that aren't helpful. We should be thinking more broadly in terms of cyberattacks, which have reached an epidemic level."

Schmidt's appointment, with regular access to the president, is one indication the government takes this broader threat seriously. Another is the acceptance by the president of the recommendations of the Cyberspace Policy Review to build on the Comprehensive National Cybersecurity Initiatives (CNCI) launched by the Bush Administration. CNCI contains a dozen initiatives aimed at establishing a front line of defense against cyberthreats, enhancing counterintelligence and the security of the supply chain for key information technologies, and strengthening the future cybersecurity environment through expanded education and R&D.

One CNCI initiative is the Trusted Internet Connections program, which aims to consolidate and secure the government's access points to the Internet.

"The goal is to create a system that looks for malicious activity at the points of connection to the public internet," says Jeff Mohan, executive director of AT&T's Networx Program Office. "The key thing is to standardize the way we do that."

Yoran, who currently serves as CEO of Netwitness, which advises large enterprises on cybersecurity, says individuals' abilities to defend themselves are challenged in the current environment. "Our adversaries—foreign intelligence services and organized crime—are using very focused cybermeans to infiltrate our infrastructures and steal intelligence and leave backdoor access opportunities for the future."

He says the government's cyberdefenses have benefited from "significant investment and attention in the last two to three years," but there is still much to do. He points to the need for increased transparency and public-private partnerships as two critical requirements.

Schmidt says much the same thing. "Transparency is particularly vital in areas, such as the CNCI, where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity," he posted on the White House web site. "In order to be successful against today's cybersecurity threats, we must [also] continue to seek out innovative new partnerships—not only within government, but also among industry, government, and the American public."

> "Transparency is particularly vital in areas, such as the CNCI, where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity."

Safer Smart Grid: Focus On A New Generation

What Will We Do If Someone Turns Out The Lights?

Government and industry alike are devoting considerable resources to making sure we don't have to ever answer that question by developing heightened security to protect a new generation of electrical "smart grids."

"There is an urgent need to establish protocols and standards for the Smart Grid," says the National Institute of Standards and Technology (NIST) in a January 2010 report.

For its part, the utility industry is expected to invest some $21 billion in Smart Grid cybersecurity by 2015, according to technology research firm Pike Research. "No utility wants to be the weak link in the chain," says Pike Managing Director Clint Wheelock in a statement.

The reason for all the attention is clear. The same technology that promises more efficient energy use through better communication between producers and consumers also opens the door to vulnerabilities, including cyber attacks, privacy theft and human error. As NIST puts it in another report, "Cybersecurity must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters."

> "There is an urgent need to establish protocols and standards for the Smart Grid."

Redundancy, Flexibility and Partnership Key to Cyber Security

By Ellen Richey, Chief Enterprise Risk Officer, Visa Inc.

As the country seeks to strengthen our cyber security capabilities, the electronic payments system is providing an example of effective partnership. Over the past two decades, payment networks have collaborated with technology companies, financial institutions, merchants and cardholders to make the payments system increasingly secure. Through their successes and failures, useful lessons about what it takes to fight cyber criminals have been learned.

First, cyber security must be based on redundancy. Consider the ways thieves can steal financial data. They can "dumpster dive" for discarded paperwork, hack computer systems or send phishing emails and text messages. There is no single solution for this multiple-front war. Instead, the electronic payments system had to develop an approach based on layers of security. These can range from the simple requirement that merchants mask card numbers on paper receipts, to sophisticated, real-time scoring technologies that analyze every Visa transaction for fraud, and most recently, mobile transaction alerts that empower cardholders to monitor their own accounts for fraud. These measures have helped the payments industry stay a step ahead of the criminals and keep fraud at low levels.

Second, every industry or government agency has its own unique needs and challenges. This requires flexibility. Rather than mandating specific, regimented technology, the payments industry advanced comprehensive security best practices in the form of Payment Card Industry Data Security Standards (PCI DSS). To date, nearly 100 percent of the largest U.S. merchants have validated compliance with the industry standards. This, combined with other industry security efforts, has resulted in fewer and less severe card data compromises at large merchants over the past few years.

Finally, the electronic payments industry has learned that security requires a cooperative approach that includes financial institutions, processors, merchants and cardholders. Cardholders can play a role in their own security by reviewing statements and notifying their financial institution of any suspicious transactions, by memorizing PIN numbers rather than writing them on their card and by treating with suspicion any unsolicited e-mail requests for financial information or other personal data.

But over the past two decades, card fraud rates have dropped by more than half and are near historic lows. This reinforces the success of applying the key principles of overlapping security, adaptability and collaborative commitment that together can help shape a strong foundation for securing our national cyber systems.

Cybercrime Is On The Move

A few numbers define the state of mobile wireless security. Forty-four percent of mobile phone users believe accessing the Internet via their phones is as safe as using their computer, according to Trend Micro.

Kaspersky Lab says that the amount of malware targeting mobile devices trebled between 2006 and 2009. Sophos found that 50 percent of mobile phone owners said their data are not protected in the event of loss or theft.

Mobile devices have lagged as cybercrime targets because no single operating system dominates, as with PCs, and there were few opportunities for scam profits. That's changing as the iPhone and Blackberry gain in popularity and Google's Android system establishes itself in the market. Sophos identified phishing applications in early 2010 targeting Android devices. Security companies like Trend Micro and F-Secure last year reported the first mobile malware bug that spreads itself by sending spam text messages. It targets devices running the Symbian S60 operating system. Kaspersky says in addition to malware, text message fraud is on the increase.

No one expects mobile cybercrime to go away. It's time for users to look into the same kind of protections for their phones as they routinely employ on their PCs.

> "No one expects mobile cybercrime to go away."

Easy Steps Keep Online Transactions Safe

It still pays to play it safe when transacting business online. Online business and finance has held up well in the current recession.

According to a new study by Javelin Strategy & Research, e-commerce grew 10.8 percent in 2009 and nearly two-thirds of American consumers say they buy things online. Estimates put the number of Americans using online banking as their preferred method at more than 50 million.

Online criminals remain active, too. Retailers expected to lose 1.2 percent of sales to fraud in 2009, according to an annual survey late last year by CyberSource Corp. This represented the lowest loss percentage in 11 years, but still a cost of $3.3 billion.

Doing business—retail or financial—online can be safe. Experts agree on a few simple steps we all can take to protect ourselves:

Only transact business from a computer you know to be secure—preferably your own. Never enter personal information—credit card or bank account numbers, PINs or passwords—into a computer with public access.

Keep your protection up to date. Make sure you are running the most current anti-virus, spyware and malware screening programs.

Know where you're doing business. Only conduct transactions with web sites you know or have strong general reputations. Look for the designation "https" in the URL window (as opposed to just "http") which indicates the site is using SSL (secure socket layer) encryption.

Be smart about passwords. Choose passwords that incorporate letters, numbers, symbols and cases, use different passwords for different web sites, and don't share passwords with anyone else. (See the related article on smart password practice.)

Use credit cards. Their issuers employ sophisticated anti-fraud detection programs. Even if your number is stolen, you may not be charged, and under federal law, your liability is limited to $50.

Social Networks Attract Crime

It's where the people are. To cyber criminals, people mean money, so the bad guys are following the crowd to Facebook, Twitter and other social networks.

According to Security Threat Report: 2010 prepared by Sophos, an IT security firm, the number of companies experiencing spam and malware attacks from social networks rose 70 percent in 2009. Nearly three quarters of firms believe employees pursuing social networking puts their security at risk. Malware, spam and trojans have been found on all kinds of social networks.

Graham Cluley, Sophos senior technical consultant says, "Social networks have become favorite hacker vehicles. They're not yet as thorough as email and search services at scanning for malicious links. And the typical person imagines he or she is in a safe place and is more likely to open a link that appears to come from a friend."

The solution is not to try to ban social network use. It's all but impossible, and the networks offer benefits for businesses. The better option, Cluley says, is to "secure and control users' access–scan every link employees click on, just like most big firms scan email."

Employees—and everyday Facebook visitors—should keep their own security up to date. Cluley recommends anti-virus software that updates itself automatically. Just as important, use common sense. Choose a good password, keep it to yourself. If someone sends you a link that seems out of character, "don't open it."

Business Model Secures Peace Of Mind

BY: JAMES LAITINEN, MANAGING DIRECTOR OF THE INTERNATIONAL INTERNET MARKETING ASSOCIATION

As technology evolves, the skill set and management of the technology results in more complexity. As complexity increases it demands a greater allocation of time and resources.

Implementation of more technology develops a logarithmic degree of risk with software, breach points, and connectivity to a wide range of digital assets. With each layer it requires its own unique and specialized resource to secure, manage, update and provide the security needed to protect your number one asset, information.

To mitigate the security risk and reduce the total cost of ownership related to technology, the best method to succeed is to leverage the business model known as managed services. A managed services provider would enable your organization to leverage highly skilled talent, at a fraction of the cost while taking advantage of enterprise grade solutions the company uses to help manage your technology infrastructure.

While some companies choose to still build their own internal solutions and systems, the problem they usually face is building a team that can scale with the organizations needs. Because a managed services organization supplies services and monitors many clients, it becomes affordable for that organization to hire and train the most talented security experts. This model of scale also allows managed services organizations to afford the best tools on the planet, and have their staff managing the needs of your business 24/7.

In this global digital economy, threats are constantly appearing around the clock. With the growing complexity and evolving threats to security, managed services is a solution that provides lower costs, expert resources, and peace of mind.

> "In this global digital economy, threats are constantly appearing around the clock."

New Capabilities Present Evolving Security Concerns

Predicting the future is always filled with fault, but a few things seem certain in cyberspace. For one, the bad guys aren't going away.

Cybercrime and the resulting need for security will continue to evolve along with the Internet itself. For another, as computing moves to the cloud, businesses and individuals alike need to grapple with new security issues.

"Security is becoming more of a business than a technical issue," says Dr. Boaz Gelbord, who recently established Security Scoreboard, the first web site to catalog and provide user ratings on online security firms. "The question you have to answer is, how much money is at risk and how much are you willing to spend to protect it?"

As cyberthreats evolve, "the least expensive aspect of most security solutions will continue to be capital purchase," according to David Lesser, president and chief technology officer of network security firm Nexum, Inc. "Ongoing operations will be the most expensive."

Lesser and other experts believe many companies make a major mistake when they assume migrating to cloud computing—where data and applications reside on the Internet rather than on a company's own servers—obviates security issues. In fact, the traditional security risks still exist—now often outside the company's direct control—and the cloud introduces new concerns to the mix.

For example, what security infrastructure and procedures does a cloud vendor have in place? Where is data stored? (It's not necessarily in the United States, by the way.) Cloud computing means shared IT environments. Your data will be stored next to other companies', perhaps even next to a competitor's. What happens if your vendor encounters financial difficulties? How is your data—and your ability to conduct business, affected in the event of a disaster or prolonged downtime?

Similar concerns face personal users of cloud-based services, such as email, photo sharing sites or social networks. They can easily expose themselves to the potential for misuse, manipulation, theft or blocked access of personal information.

Moving forward, the benefits of using the cloud will continue to be compelling. Users need to develop a clear view of the security issues involved.

> "Other experts believe many companies make a major mistake when they assume migrating to cloud computing, where data and applications reside on the Internet rather than on a company's own servers, obviates security issues."

Product Review: Encrypt-Stick™

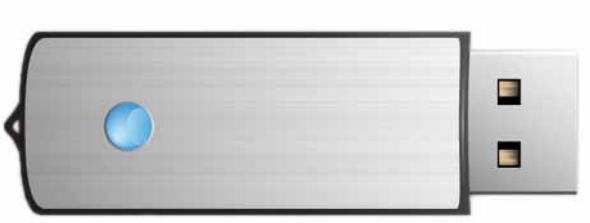
Encrypt-Stick

Turn Your Flash Drive Into A Data Fortress

Simplicity—that's one of the many appeals of Encrypt-Stick, an inexpensive, easy-to-use application that provides maximum protection for your data—using only a USB flash drive. Encrypt-Stick employs powerful 512 bit polymorphic encryption technology and three unique variables to build an impenetrable vault for your data. Encrypt-Stick is a downloadable software that runs on any serial numbered USB flash drive for a modest $39.99 fee. Encrypt-Stick marries a unique registration number with the flash drive's serial number and a password you create and only you know. You can encrypt documents, files, photos and videos by simply dragging and dropping them into an invisible vault (encrypted folder). Once encrypted, the file can be placed on your desktop or network, transferred to a CD or DVD, or emailed to another computer—but it cannot be opened and read without the Encrypt-Stick enabled flash drive that encrypted the file.

Encrypt-Stick's designers included several useful features. Once you encrypt a file, the software erases the original (if required) and leaves no trace for data recovery programs or forensic software. Encrypt-Stick key offers a "Lost Flash Drive Utility" in the event of a lost or stolen flash drive. Encrypt-Stick also includes a Password Manger function for encrypting all your passwords, web addresses, banking and credit card information, and email logins. The only password you need to remember is the one you created for your Encrypt-Stick enabled flash drive. Password Manager will even rate the strength of current passwords and produce maximum-strength alternatives, if required.

Your Encrypt-Stick enabled flash drive provides not only data encryption, but data protection and peace of mind.



Q & A

Cyberbullying

PARRY AFTAB
Executive Director
WiredSafety

Cyberbullying is a growing problem. One nationwide poll of 45,000 middle school students found that 85 percent had experienced cyberbullying.

We asked Internet privacy and security lawyer Parry Aftab, executive director of WiredSafety.org,. for some common sense advice.

Q: What constitutes cyberbullying?

A: Our simple definition is the use of digital techniques as a weapon to hurt, embarrass or intimidate someone else.

Q: What can parents do to prepare their children?

A: First, recognize your child can be the bully as well as the victim. That's hard to accept, but the progression online from disagreement to flaming to bullying happens quickly. Often it's the last click of the mouse that decides. Second, don't keep kids off the Internet. Lots of kids who don't even have Internet connections have been victims. Third, teach kids to turn to a trusted adult (preferably parents) and realize that as parents, we have to earn that trust, primarily by not overreacting. Fourth, on a very practical level, teach your kids never to share passwords. Surveys show most kids do. When friends fall out, those kids are vulnerable to all kinds of online attacks.

Q: What do I tell my son or daughter to do if they are bullied online?

A: Three things—stop, block, tell. The first is the most important. Don't react to the initial provocation. Put down your mouse, go offline, do something else you love for at least five minutes. (We call that "Take 5!") Second, block the bully or the message. Third, tell your parents (or another trusted adult) what happened. Let them help.

Q: Where can parents go for help?

A: If the situation is dangerous, you have to go the police. Short of that, parents will find help and a wealth of resources at WiredSafety.org and our StopCyberbullying.org.

Cyberthreats

AMIT YORAN
CEO, Netwitness

Q: Who's most at risk, government or the private sector?

A: Both face similar challenges in terms of the nature of threat, methods of attack and pervasiveness of compromises. The biggest danger is believing that your organization is not a target. Over the past several years, we've seen state sponsored attackers and organized cybercriminals attacking government and private systems with equal vigor. Their pursuit of information or financial gain has not limited their activities to sophisticated intelligence agencies or large financial institutions.

Q: What's the biggest threat organizations face?

A: Gaining awareness of what's going on in their IT environments. The biggest failure is assuming that because no alarms are going off, your environment is safe. Over the last two decades, the security industry has relied almost exclusively on signature-based products—security tools that look for electronic signatures or patterns of known bad behaviors. For the last three to five years, our adversaries, both nation-state and organized crime, have professionalized and customized their means of attack. They're no longer using generic attack methods for which well known signatures exist.

Q: What do organizations need to do?

A: On a practical level, tighten control of your IT environment. Restrict access, lock down the infrastructure and maintain good hygiene. These actions won't keep advanced-threat actors out, but they will start reducing the volumes of system compromises so that you can identify the sophisticated threats. Use automated means to leverage threat intelligence. Apply forensic rigor in your analytic processes. Prepared organizations can identify and respond to incidents effectively and minimize loss.

Amit Yoran served as director of US-CERT (Computer Emergency Readiness Team) and the National Cybersecurity Division of the Department of Homeland Security. He is now CEO of Netwitness, a cybersecurity firm with both public and private sector clients.

Cyberdefense: Start With A Good Password

No component of online security is more critical—and receives less attention—than passwords.

A strong password is the lock on the door that secures personal information at countless web sites, yet millions choose combinations that are child's play for hackers. Two favorites are "1234" and the word "password" itself. Many people choose the name of their computer monitor. Others select the name of their pet—which they also post on their Facebook page.

Following a few simple rules can greatly enhance password—and online—security. Don't use words found in the dictionary. Hackers have automated programs for those. Avoid personal information. The longer and more complicated the password, the better. Use the whole keyboard. Don't forget to use upper and lower case letters, numbers and symbols. Each additional element vastly increases the potential permutations and combinations. Don't use passwords on public computers. If you need to write a password down, keep it in a secure place. Above all, don't share passwords with others.

Graham Cluley, senior technical analyst for Sophos, an IT security firm, recommends starting with a phrase you can easily remember then reducing it to a meaningless string of characters. For example, "Don't be late for staff meetings Tuesday mornings at 9:00" becomes "Dbl4smTm@9."

Never use a single password for more than one website. Several online applications will do the work of remembering multiple passwords for you.

Password practice is more time and trouble but a modest price to pay for the enhanced security that results.

Leveraging Your Career In Cybersecurity

There's little doubt as to the need. The White House's Comprehensive National Cybersecurity Initiative (CNCI) states it right up front in Initiative #8: Expand Cyber education.

"There are not enough cybersecurity experts within the Federal Government or the private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field."

Professor Eugene H. Spafford, who heads the Purdue University Center for Education and Research in Information Assurance and Security, told a Senate committee last March, "We need significant, sustained efforts in education at every level to hope to meet the challenges posed by cybersecurity and privacy challenges." He cited estimates of financial losses to due cybersecurity breaches in the tens of billions of dollars.

Educational institutions are moving to fill the void. Virginia College, for example, offers a Master of Cybersecurity degree, designed to provide in-depth study in IT infrastructure security, through its online program. Numerous other colleges, universities, and educational consortia, offer undergraduate and graduate curricula in network security, computer forensics, cyber law and related subjects.

One silver lining—at a time when jobs are hard to come by, the growing need for trained experts who can help fight the bad guys in cyberspace offers seemingly unlimited opportunity.

Panel Of Experts

STEPHEN BALKAM
Founder and CEO
Family Online Safety Institute

The Family Online Safety Institute is an international, non-profit membership organization dedicated to making the online world safer for kids and their families. FOSI works to identify and promote best practices tools and methods in the field of online safety that also respect free expression.

There is no silver bullet to protect children from the risks of digital media. A combination of education, awareness, tools and rules will help guard children from harmful content and will empower them to act responsibly online. FOSI promotes a culture of responsibility online, where different, but overlapping layers of society work together in a coordinated effort. These layers include reasonable government oversight, enlightened law enforcement, self-regulated industry, tech savvy teachers, empowered parents and resilient kids all working together to make wise choices online.

As broadband is expanded into new homes, it's now more important than ever to make the web a safe place for families. We need a broadband responsibility program in place before, during and after broadband rollout to help foster digital citizenship in the online world. FOSI is currently working on a broadband responsibility program and continues to be dedicated to making the Internet safer for families as we connect the next billion people online.

RICHARD C. SCHAEFFER, JR.,
Director, Information Assurance
Directorate, National Security Agency

NSA supports the Nation's interests by protecting and defending National Security Systems and assists with the protection of information in cyberspace. In collaboration with the Department of Homeland Security, we assist National Security and other U.S. Government clients who have the responsibility to protect the Nation's critical infrastructure. NSA's Information Assurance mission ensures the availability of products and services that enable our clients and customers to execute their operations in the face of constantly increasing full-spectrum adversarial activity. Our partnerships with military commands, allied governments, and U.S. industry reflect the extensive community collaboration that is the cornerstone of operating more securely in the global network environment. No one department or agency can go it alone, nor can any one agency provide all the capabilities necessary to counter today's cyber threats. We apply our unique knowledge, skills, and abilities to understand how technology can fail, or be made to fail; develop measures to mitigate these vulnerabilities; define security standards and best practices; and foster increased automation of mitigation technologies and techniques. NSA also supports cybersecurity education and academic research, activities critical to expanding the workforce deemed essential to meeting the Nation's challenges in cyberspace.

JAMES MOBLEY
President and CEO
Neohapsis

Cybersecurity is one of the most critical challenges that our nation will face during this decade. Information security experts, armed with advanced technologies, will play a key role in our ability to meet this evolving challenge. However, while acknowledging that we will never be 100 percent secure, most in our industry agree that an effective solution for securing cyber space must focus not only on response but, more importantly, on prevention. Central to a prevention strategy is developing a risk aware organization at every level of the enterprise. Simply stated, the best performing companies and organizations anticipate and navigate risk better than the laggards.

The pursuit of risk management excellence is accelerated when a Governance, Risk and Compliance, or GRC framework is in place. Effective GRC systems leverage a single software platform to monitor and enforce rules and procedures. These systems also bring visual clarity to the relationships between business objectives, risks and operational controls. When the impact and interdependencies of each risk is known, prioritized and managed holistically, an organization is best prepared to avoid the downside of risk, as well as capitalize on the opportunities that risks also present. Secure principles embodied within a comprehensive GRC framework is a winning combination.

TODD DAVIS
CEO
LifeLock

Recently, the Federal Trade Commission reported that over 100 organizations have improperly released sensitive consumer data on file-sharing networks. These networks, referred to as peer to peer (P2P), are used every day by consumers to download music, videos and documents. Unfortunately, identity thieves are also using the P2P technology and black market web sites to steal identities.

If a consumer's personal information is released on any of the P2P networks or Web sites, an identity thief can download the information to commit the crime.

LifeLock can help protect this sensitive information from being misused. LifeLock eRecon Service searches the web for illegal selling or trading of personal information. If eRecon Service detects any activity, LifeLock will alert the member and help the individual take steps to resolve the problem. In addition, LifeLock has a $1 Million Total Service Guarantee. If a member becomes a victim of identity theft due to a failure in LifeLock service, LifeLock will help fix the issue at the company's expense up to $1 million. (Restrictions apply. See lifelock.com for details. Due to New York State law restrictions, the LifeLock $1 Million Total Service Guarantee cannot be offered to the residents of New York.)

LLOYD R. MEESE
CEO
Wi-Ex

As a leader in wireless communications, we know firsthand the impact poor in-door cell phone signal has on today's mobile consumer especially when it comes to personal safety and emergencies. According to our zBoost "State of the Cell Signal" Survey, commissioned by Wi-Ex , and conducted by Harris Interactive, nearly 70 percent of cell phone owners consider their cell phone their essential communications tool and 67 percent of owners experience problems with their cell phone signal at home.

With an increasing number of Americans opting to drop their landline and relying solely on their mobile phones, a reliable in-door cell phone signal is essential. Our products can help in a variety of areas for both personal and public safety including disaster areas, campuses, health care facility, safety and emergency vehicles, as well as public parking decks. Often in disaster areas a cell phone is the only communication to the outside world. Our customers and dealers have shared their stories from using the zBoost to stay connected following hurricanes to most recently our dealer, Quantum Wireless, using a zBoost connected to a wind turbine during a mission to Haiti. Our zBoost products can help cell phone users stay connected during these difficult times.

Knowing is the Key to Protecting

By: NetWitness Corporation

There is a great deal of debate taking place about whether or not we are engaged in a cyber-war. Some disagree with the terminology because of the legal and policy implications. Others argue that the sensational nature of the term spreads fear, uncertainty and doubt or raises hysteria. Regardless of what we call it, the facts remain uncontested. Criminal and nation-state adversaries continue to compromise systems and steal information on a regular and large-scale basis.

The security technologies which government and industry relied upon for the past few decades are not keeping us safe.

The security technologies which government and industry have relied upon for the past few decades are not keeping us safe. At their core, these technologies depend on prior knowledge of what bad behavior looks like and require electronic signatures to know what to target.

Today's adversaries, whether state actors or criminals, are relying on advanced threats. They show focused intent on compromising targeted systems because money or national interest is on the line. They organize complex campaigns when necessary, frequently relying on a high degree of technical acumen and custom attacks or exploits to break into their targets. These attackers put forth the effort to test their methods to assure they do not trigger the well-known signature sets of intrusion detection systems and anti-virus products.

A focused adversary with intent and time will compromise even a well-defended enterprise network. There are simply too many opportunities for unauthorized access, too many ways to exploit systems, too many uncertainties about what vulnerabilities exist in your infrastructure. Modern attacks hide themselves in your users' applications – they look like normal web traffic, email attachments or PDF documents. Once they compromise a system they allow outsiders to target and steal information, access login credentials and exfiltrate large volumes of data and covertly command and control the system remotely.

If you're relying on the signature-based approaches of 1998 to protect you against these modern threats, you're operating blind to the threats that matter most. This does not have to be the case. While you can't provide absolute security to your environment, you can shed the fear, uncertainty and doubt that envelope you today.

There is a solution that can provide the knowledge you need to protect your organization. Know exactly what's going on in your network. Know what communications and applications are coming into and out of your environment. Know where advanced methods are being employed to bypass security technologies. Know when new exploits are attacking your systems. Know when these attacks have been successful in compromising systems. Know what the patient zero of any compromise is and what vector of attack was used. Know when your systems are being controlled from the outside. Know what the scope and size of a security breach really is. Know exactly what data has been exposed and exfiltrated.

With NetWitness, you can finally stop feeling like a victim and worrying about the unknown. Start knowing more and get used to feeling protected again.

www.netwitness.com