A LOOK AHEAD

A group of prominent security professionals forecast the most significant industry shifts in 2013. Greg Masters compiles the responses.

Q: What threat vectors will be most prominent? Why?

Winn Schwartau: Mobile. Without question, mobile.

Jarno Limnéll: The world will experience more intentionally caused cyber attacks, and international debate on using cyber space for different purposes will increase. The development of highly sophisticated malware by state-sponsored organizations has the potential to radically affect the speed at which the wider threat landscape evolves. Cyber threats will be more unpredictable than ever before. Nations-states are taking cyber espionage more seriously, and accusations between countries will rise to more severe levels.

Steve Durbin: Today, we're seeing that C-level executives are increasingly being tasked with managing a widening range of company security risks. Most IT business decision-makers are not necessarily dealing with daily catastrophes, but are dealing with the challenge of creating a stable environment to reduce risk and the associated costs of doing so. But when things do go wrong, security challenges do occur. A thorough understanding of what happened and why is necessary to properly understand and respond not just to the incident, but also to the underlying risks associated with that incident.

George Bilbrey: The social engineering of email is a prominent threat vector. Email is becoming more attractive due to mobile – all of the education around how to identify phishing and spoofing messages only applies to a message seen on a desktop or in webmail. On mobile devices, all bets are off. Additionally, mobile consumption tends to be quick – users aren't taking the time to check email over closely to tell if it's phishing, increasing its effectiveness. And phishers are optimizing for mobile. In fact, it's actually easier for spammers and phishers to make an email message look legitimate on a mobile device.

Daniel Kennedy: Mobile is a chief concern for most of the security managers I speak with, and there's little doubt why, with the flood of employee-owned devices coming into their firms' systems environment. It speaks, in a larger sense, to the evolution of what will be the endpoint of the future, as what are now separate mobile device management and mobile application management and mobile security applications will converge as mobile devices potentially meet or overtake PCs as the primary business computing device.

> "We anticipate continued evolution of exploit kits..."
>
> —Rob Kraus, Solutionary

Rob Kraus: We anticipate continued evolution of exploit kits and deployment of malware through targeted attacks, as well as an increase in the visibility to malware distributed via mobile platforms. Several significant advancements have been noted to the advanced exploitation capabilities and deployment of BlackHole Exploit kit, as well as other similar platforms.

Ryan Hurst: This year we saw a trend develop where foundational technologies on the internet that have been treated as largely solved problems became attack vectors. As we look at these issues, in every case we see that they could have been easily prevented by following industry best practices for use of the

Our panel of PROGNOSTICATORS

Nick Cavalancia
is SpectorSoft's VP of marketing.

George Bilbrey
is co-founder and president of Return Path.

Steve Durbin
is global executive vice president of the Information Security Forum.

Jeff Hudson
is CEO of Venafi.

Ryan Hurst
is the chief technology officer at GlobalSign.

Daniel Kennedy
is a former Wall Street CISO and current research director of information security at 451 Research.

Rob Kraus
is director of research, Solutionary Security Engineering Research Team (SERT).

Jarno Limnéll
is director of cyber security at Stonesoft.

Winn Schwartau
has appeared before Congress as an authority on cyber security, and has been a regular speaker at industry events, including SC Congress and DefCon.

Suzanna Schmeelk
is a network security research scientist at LGS Innovations - Bell Labs in New Jersey.

Tatu Ylonen
is CEO of SSH Communications Security and the inventor of SSH.

QUICK TAKE: What's ahead in 2013?

	Will security budgets increase, stay stagnant or decrease?	Will any significant security-related legislation (or executive order) become law?	What "emerging threat" will finally break out and become a real risk?	Will we be any more secure by December 2013?
Winn Schwartau 	Increase by 12 percent.	Probably some version of Compliance Inspection.	High-energy radio frequency (HERF)/ electromagnetic pulse (EMP).	A lot less.
Jarno Limnéll 	Most security budgets will increase slightly unless the company was recently breached. Then, they will spend more.	At this moment, it seems that within the next year security legislation that would dramatically change the current situation will not be executed.	I am afraid that we are not far from the situation where bytes will cause serious damage to the physical world (to civilian society), and that will have significant consequences.	I hope so – both in security as a feeling and because of real actions to prevent threats.
Steve Durbin 	While budgets may remain the same or even increase a little, there will be an ever-increasing number of calls on those security budgets.	Expect the Europeans to continue to bring into force legislation across the EU targeting privacy and use of data, while in the U.S. any talk of executive orders will likely depend on the outcome of the presidential elections.	I don't expect to see any one particular emerging threat take over the limelight. What is more concerning is when threats collide to create "superthreats".	The pursuit of "secure" is an unrealistic goal – I think we may well see us being more resilient; that is, better equipped to handle and deal with emerging threats that we encounter.
George Bilbrey 	They will increase. Companies see the headlines when a data breach or attack occurs, and no one wants to be on the wrong side of that.	No, not this year.	Spear phishing is likely to become more widespread, especially since it only takes a few "hits" for the criminals to be successful. These attacks often target high profile individuals and hit them where they are weak.	Yes, because ISPs are doing more to protect their networks, companies are finally starting to pay attention to the need to protect their brands, and users are becoming more aware of threats because of increased media coverage of scams and better user education.

associated technologies. In several of these cases, the vulnerabilities that were being attacked were known for nearly a decade, and mitigations existed, yet they were still ignored. Recent examples include Flame.

I believe we will see this trend continue in 2013 because I have not seen the industry put in place the processes, procedures and toolsets that are necessary to address these risks.

Nick Cavalancia: By far, the greatest threat to security and compliance is BYOD. With no control over personal devices that have access to company data, applications and critical systems, organizations that are adopting BYOD are creating the greatest gap in their security model.

With BYOD, it will be easier than ever before for data to leave the organization, whether it be maliciously via a forwarded email, for example, or accidentally via lost or stolen tablet devices. These are just two examples – there are (and will prove to be) many more in 2013.

Suzanna Schmeelk: I think the rise of cloud computing will see an increase in novel threat vectors, particular related to data leakage and denial-of-service, because attackers usually want information or want to deny other people service.

Tatu Ylonen: Engineered cyber warfare viruses. The Pandora's box has been opened, and "everyone" is scrambling to do their own.

Jeff Hudson: Attackers will escalate their assault where they find weak encryption keys and mismanaged certificates. Every enterprise relies on hundreds and even thousands of certificates and encryption keys, but few know where each one is and how they're used. Criminals know this and have only just begun their attacks. The techniques used by Stuxnet, Flame, and Duqu are now in the hands of common criminals and will be used for intellectual property theft and inflicting serious harm on enterprise systems.

Q: What security solutions/services will see increased adoption? Why?

WS: More intelligent SIEM and visualization.

JL: An increase in telemetry allowing visibility by geographical IP (country) in SIEMs, as well as more proactive policy-driven incident response efforts will be a focus.

GB: Both ISPs and brands will increase their adoption of reporting back incidences of abuse or fraud against their users and brand. The use of DMARC and other aggregated real-time reporting are effective ways to stop phishing messages and password compromises.

DK: Mobile device management (MDM), endpoint/network data leakage prevention (DLP) and application aware firewall implementations will see the greatest percentage of greenfield implementations.

RK: Monitoring and DLP implementations will continue to rise due to organizations' desire to identify attacks and establish visibility into potential breaches.

RH: We have had a number of practical attacks relating to poor cryptographic key management and the use of cryptography in security. I believe this has raised the visibility of the importance of these topics and as such we will see a move to better manage the associated risks.

Additionally I believe recent attacks have shown that authentication and privacy is more fragile than customers often realize.

As a result, I believe we will see increased adoption in knowledge-based, continuous best practices assessment tools and guidance, cryptographic key management solutions, strong authentication technologies, and privacy-enhancing technologies such as SSL.

NC: Employee monitoring is on the rise. With IT's job of securing environments becoming more complex with the inclusion of BYOD, social media, cloud computing and Big Data, organizations are realizing they are losing control over how employees get their jobs done.

> "The rise of cloud will see an increase in novel threat vectors."
>
> —Suzanna Schmeelk, LGS Innovations - Bell Labs

SS: I think more hardware-based security solutions will see increased adoption.

TY: Security must increasingly be preventive. A properly engineered virus will have run its cause within five minutes from first activation. Much of the spread will happen within 20 seconds. No human-mediated response will be fast enough. In this time the virus can destroy modern society.

JH: Security solutions that allow enterprises to proactively identify weaknesses and coordinate a response will continue to see increasing demand. For management, auditors, and regulators, it's no longer acceptable simply to detect a vulnerability or attack in progress.

Q: Which will see declining adoption rates? Why?

WS: Password enhancement tools in favor of stronger authentication.

JL: More commoditized solutions that aren't necessarily ported directly to the virtual environment may be in decline but still are necessary, including anti-virus, anti-spyware, etc.

GB: Microsoft made a good attempt with SenderID, but it's unlikely anyone will be using it going forward. Both brands

QUICK TAKE: What's ahead in 2013?

	Will security budgets increase, stay stagnant or decrease?	Will any significant security-related legislation (or executive order) become law?	What "emerging threat" will finally break out and become a real risk?	Will we be any more secure by December 2013?
Daniel Kennedy 	For the plurality of firms, security budgets are increasing in 2013, largely in the range of a five- to 10-percent increase.	One thing that is very difficult to predict is the potential efficiency of Congress in getting anything passed. No less than our secretary of defense has demanded action on cyber security noting a serious existential threat to the United States critical infrastructure, yet the *Cyber Security Act* can't even be brought to the floor for a vote.	We're likely to see more widespread attacks on dual-factor authentication implementations, both as they become more commonplace as a protection for online financial transactions and as mobile devices become more common as the second factor (the "what you have") to the authentication process.	A concern I have is the amount of security investment that still appears driven by compliance audits, which in turn appear driven by media coverage of significant security breaches.
Rob Krauss 	Stagnant. Many organizations will not increase budgets until they are in the crosshairs and have suffered a major loss in revenue due to a breach.	It is hard to say for certain, but there are many areas to focus based on different vertical markets. Compliance initiatives will continue to mature, and through publication of major breaches occurring in the public sector, the government will likely step in to start enforcing more and provide guidance.	We are going to see an increase of cyber war capabilities and operations between nations. Great efforts have been initiated to "ramp up" cyber defense and offense capabilities, and it will soon be realized that these tools can be effective and efficient.	We can only hope. However, security is a culture, and the culture of security will take a long time to mature to see the shift to having a "security first" mindset.
Ryan Hurst 	I believe they will increase to a great extent due to the need to increase the size of the security teams themselves.	Worldwide certainly, but we will see further security-related legislation here as well.	Poor key management.	Security is a process, one we are getting better tools and processes for every year. I do believe we will be more secure, but given it is a process, the risks will continue to evolve and we will need to evolve with it.

and ISPs are going to stick with sender policy framework (SPF) and DomainKeys Identified Mail (DKIM) because of domain-based message authentication, reporting and conformance (DMARC).

DK: Once in place, few security solutions ever decrease in adoption. The greatest negative is usually stagnation in growth. Solutions that seem to have a hard time growing include tokenization solutions (despite a PCI compliance related push); network access control (NAC), which may largely be getting subsumed into other security solutions; and dedicated anti-spyware solutions as firms look to more comprehensive endpoint security suites.

RK: Instead of me stating what will decrease, we should focus on what should decrease. The top on my list is signature-based detection of malware. Organizations should focus on anomaly-based detection and heuristics supporting detection of attacks and malicious code. Signatures have their place in detection, but solely relying on them to be the primary detection mechanism is something we as an industry need to move away from.

RH: This year we saw several examples of highly advanced malware developed for military purposes spread more broadly than we believe their creators had intended. As governments begin to develop effective and formal cyber defensive and offensive programs we can expect to see more examples of the same.

SS: I don't think adoption rates will decline as much as adoption rates will become transparent and unnecessary from the personal user's perspective. For example, many old services are becoming configured correctly right "out-of-the-box," so the average user needs not worry immediately.

JH: Across the board, point security products that require more time to manage and maintain are on their way out. There's just not enough time in the day for teams to keep doing more. Whether it's an IDS, firewall, encryption, or analytics product, if it requires more administrative time to oversee rather than reducing workloads, the technology is sure to see to declining use and slower adoption.

> "Signature based systems will become generally less effective."
>
> —Ryan Hurst, GlobalSign

Q: Which security lessons will organizations be forced to learn this year? Why?

WS: Co-mingling personal and corporate data on a mobile device is a lawsuit waiting to happen.

JL: The most important lesson: Cyber security is primarily a strategic issue. The digital world has become a domain where strategic advantage (national, industrial or military) can be lost or won. Strategic understanding and guidance for technical solutions are needed more than ever before.

SD: More organizations will fall victim to information security incidents at their suppliers. From bank account details held by payroll providers to product plans being shared with creative agencies, organization's data is increasingly spread across many parties. While the IT function can, in theory, provide an inventory of all data they hold, it is difficult to do that throughout the supply chain. The risk is complex.

DK: Organizations will continue to learn that security programs start with a dedicated senior executive leader for information security independent of the CIO, head of compliance, legal, or anyone else. A casual approach to the influx of employee-owned mobile devices accessing company resources will keep generating problems for the firms that allow it, from data leakage to arguments about who owns the device when a forensic investigation is required. Advanced or adaptive persistent threats, depending on what you want to call advanced motivated attackers, will continue to drive home the message that a good security program is a balance between preventative controls and incident response processes, and there is no one-time, hands-off, tool-dependent approach to information security that will be effective.

RK: I believe that as more details unfold about targeted attacks, organizations will have a better view to understanding that attacks are no longer focused on one vulnerability, but are three-dimentional in nature. Attackers are becoming more proficient at coordinating attacks, leveraging social media, crowd-sourcing and instilling fear in even the largest of organizations. No organization is safe, and preparation is key to effective defense and mitigation.

RH: In some respects, we will see the renaissance of security in 2013. To address the risks, one needs to develop and use formal security assurance programs. Such programs allow customers to continuously review the deployment practices and the configuration of the systems they both use and develop. This is especially true as we see broad movement to the rapid development model that software-as-a-service enables. As a result, I believe organizations will be forced to refocus on how they accomplish their business goals securely with the new realities we live with.

NC: With notification firmly in place, organizations will be forced to take security and compliance far more seriously, or they will literally pay the price. Organizations are going to have to accept that lost and stolen computers can be protected with file-system encryption, that internal fraud can be reduced with

QUICK TAKE: What's ahead in 2013?

	Will security budgets increase, stay stagnant or decrease?	Will any significant security-related legislation (or executive order) become law?	What "emerging threat" will finally break out and become a real risk?	Will we be any more secure by December 2013?
Suzanna Schmeelk 	I think budgets will increase. I do think savvy management can temporarily compensate for stagnant budgets.	I think the EU is still way ahead of the United States as far as privacy laws are concerned. I'm particularly impressed with the EU's opt-out laws. I would like to see deeper electronic privacy laws protecting humans.	I think our homeland infrastructure needs more protection.	Yes. Enlightenment by default improves security.
Tatu Ylonen 	I read from various sources they will decrease. This is concerning.	Yes, I believe new cyber security legislation will advance. The election results provide continuity to speed up the process.	Unmanaged SSH keys.	Yes, but it will not look like that because threat pressure will likely increase and become more sophisticated.
Jeff Hudson 	All signs indicate that most IT security budgets will grow in 2013. Both the increased attention to breaches and security teams doing a better job articulating both risk and business value are helping to grow security budgets. Security projects that can help accelerate these strategic projects and reduce work elsewhere are certain to have the best chance of being funded in 2013.	It's unlikely in 2013 with major showdowns over the U.S. budget, taxes, and entitlements that new cyber security or data protection legislation will be enacted. However, new executive orders that address preparedness and government sharing, as suggested by former White House Cyber Security Coordinator Howard Schmidt, are likely given the their relatives ease of enacting. Globally, it is possible that an update to European Data Protection Act will usher in EU-wide data breach notification and more consistency across countries.	Look for attackers to increasingly turn mismanaged security back on enterprises. Attackers will turn security controls that every enterprise relies upon, like encryption and certificate based authentication, against organizations. Whether it's a weak cryptographic algorithm or a certificate from a compromised CA, cyber criminals are fully aware of how to leverage this vector and they know that organizations aren't prepared to defend against it.	Looking at the "hockey stick" growth in malicious code, rise of cloud computing, and rampant use of mobile devices, one thing is certain in December 2013: Enterprises will have more risk to manage than they did at the beginning of the year, especially those enterprises that are embracing innovation. So are you safer and more secure in 2013 if you're in an organization that doesn't embrace change? No.

employee-monitoring software and that employee data theft can be curbed by controlling BYOD.

Solutions exist today that provide answers and, in some cases, are even part of the very operating systems in place.

SS: I think security will become more of a service when organizations recognize the cost of potential business loss.

TY: Automated access to servers must be taken into account in identity and access management. Many organizations now have more automated trust relationships between computers than they have interactive users. For example, one study we did found over a million SSH user authentication keys in a bank with "only" 200,000-300,000 employees. Security professional and business leaders are likely to learn that the cloud is no longer for test projects. Accountability for cloud security and compliance begins and ends with the enterprise alone.

Q: What will be the most surprising security-related development?

WS: That BYOD is complete epic fail.

JL: Most surprising is the financial DoS and DDoS events that have taken place recently. These are some of the largest institutions that are most heavily regulated. It goes to show how important research and development is from a cyber security perspective to ensure a proactive, ever-evolving and layered defense-in-depth strategy regardless of the existing controls. Its very much moving toward an offensive/countermeasures environment today.

GB: Cyber crime is going to continue to move past financial services into other kinds of big brands and institutions. Criminals are probing for new ways to get malicious messages through. This year, brands and institutions that we haven't previously considered vulnerable will be threatened.

DK: After the revelation of a potentially U.S.-sponsored cyber attack on a foreign nation's nuclear program, the ongoing evidence of foreign nations' infiltration into our own computing infrastructure, attacks by chaotic actors into security company IT environments, the disintegration of the 'trust infrastructure that the internet's own communication is pinned upon, and the continued commoditization of mercenary-style cyber attacks, it's hard to be surprised anymore. Expect more of the same, especially as IT executives continue to mix an uncomfortable casualness with an increasingly complex technology environment, with mobile and cloud being notable aspects of this complexity in 2013.

> "BYOD is complete epic fail."
>
> —Winn Schwartau, authority on cyber security

RK: Well, if I let that out of the bag, it wouldn't be a surprise, would it? Honestly, there are so many advancements in both attacker and defense capabilities it is hard to put a finger on what will be most surprising. Last year we saw a rise in attacks via hacktivism and a lot of focus on the financial sector. I believe over the next year we will continue to see those types of activities, the amplification of SCADA-related attacks and focus on pointing out gaps in security versus compliance.

One large surprise would be if the security cultural shift was focused more toward being secure, as opposed to being compliant. Organizations who focus on being secure, applying security where appropriate, and have executive management support for their organizations' security programs will ultimately fare much better during an attack than those who simply aim to meet compliance directives.

RH: One thing that security teaches us is to be pragmatic. As a result, it's difficult to say anything is surprising anymore given so much of what we do can be described as defining and following best practices, yet we continuously see people failing to do so.

What I am unsure of is how the government's investments in cyber security will shape how we secure our systems and how security incidents are handled.

JH: Many pundits, leading media outlets and security experts have been reporting that enterprises needn't be overly concerned about Flame-style malware attacks as they were executed by advanced espionage organizations and aimed at hostile governments in order to gather intelligence. Unfortunately, the tools and techniques for executing these type of attacks are now in the hands of common criminals, not just the most advanced intelligence agencies. In the coming year, this same type of attack is going to be perpetrated against major enterprises. In fact, the breach may have already occurred. ■