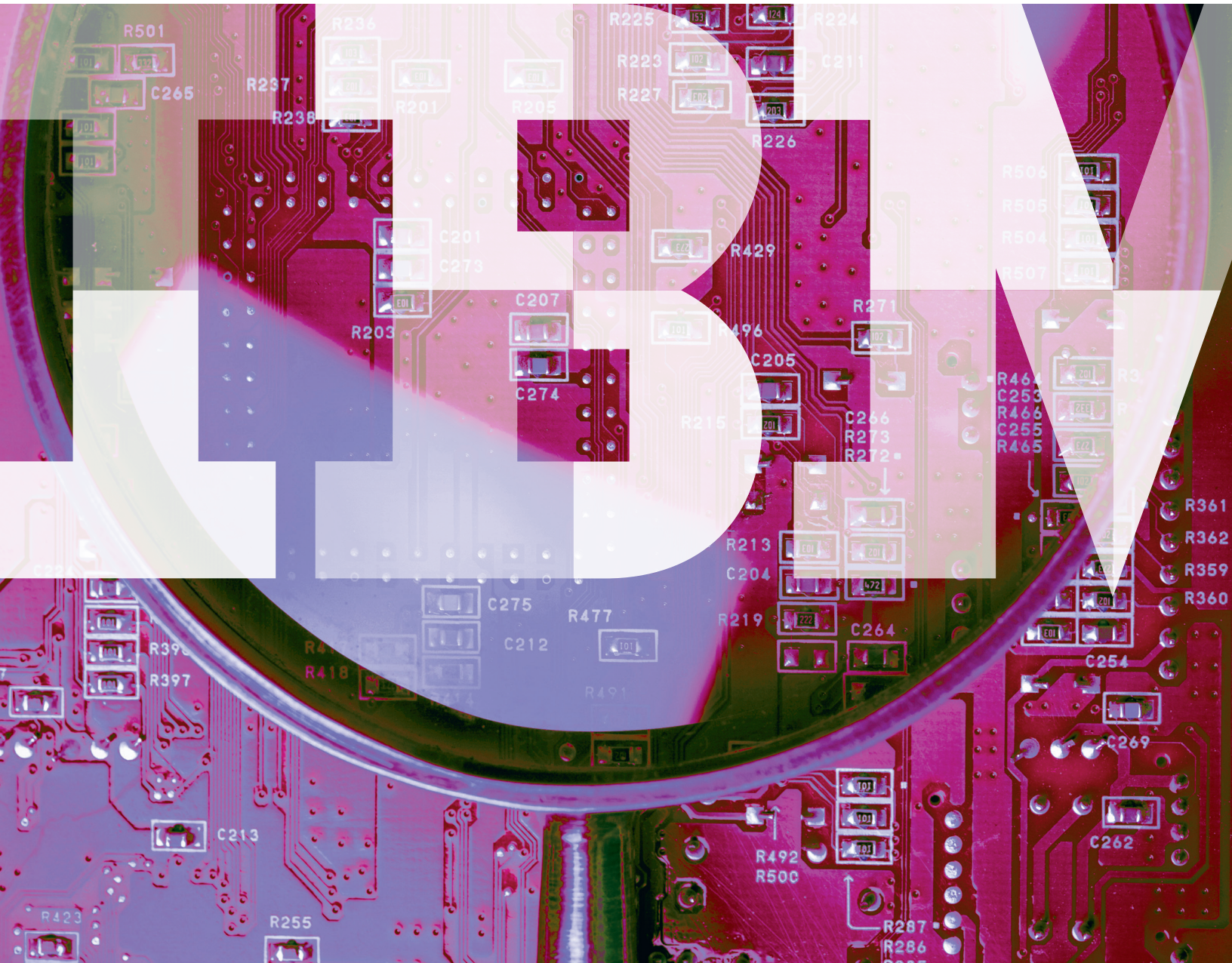
IBM Institute for Business Value

Emerging security trends and risks

Insights for the business executive



IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive report is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value.

You may contact the authors or send an e-mail to *iibv@us.ibm.com* for more information. Additional studies from the IBM Institute for Business Value can be found at *ibm.com/iibv*

By Jack Danahy, John Lainhart and Eric Lesser

2011 was a remarkable year for IT security.

The frequency and scope of data loss, "distributed denial of service" attacks (preventing legitimate users from accessing a service) and "social hacktivism" (using computer networks for social or political protest) reinforce the need to protect assets in an increasingly connected world. Because it is unrealistic to avoid new connection-enabling technologies, business executives can address emerging security risks by: building a proactive security intelligence capability; developing a unified view of all endpoints, including mobile devices; protecting information assets at the database level; and creating safer social habits.

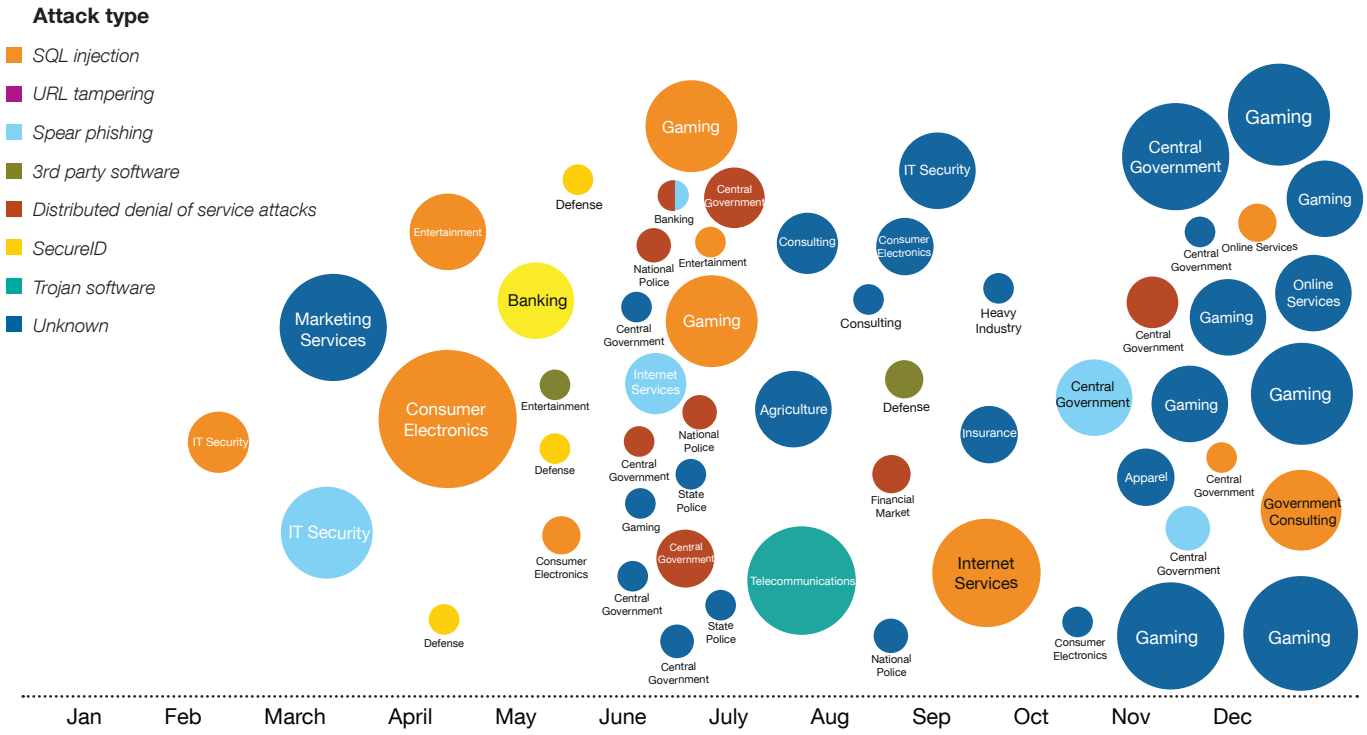
The 2012 IBM Global CEO Study reveals that leaders are recognizing that our new connected era is fundamentally changing how people engage with employees, customers and partners.[1] As individuals and organizations become parties to more connected, open, mobile and social forms of commerce, new approaches to exploitation are being devised. Not only are these attacks targeting information technology and infrastructure, but individual users as well, taking advantage of basic human nature. As a result, security can no longer be a discussion that remains within the domain of information technology professionals. Rather, protection in this new environment requires the understanding and vigilance of individuals at all levels of the organization.

Many of the traditional security threats that have been prevalent over the last several years are continuing to evolve and spread.

The IBM X-Force, a team of vulnerability researchers, continually monitors and analyzes security threats around the world and publishes its findings on a twice-yearly basis.[2] This wealth of data provides a unique, first-hand view of the current issues and challenges in cyberspace. The implications of this data have repercussions not only for the IT professional, but for the business executive as well.

2011 was marked by frequent, wide-scale network security breaches, leaving a wake of leaked customer data, inaccessible web services and billions of dollars in damage. These incidents did not discriminate against any single industry or sector; law enforcement, governments, social network communities, retail, entertainment, banks and non-profits all reported notable attacks (see Figure 1).

In this report, we will discuss a number of specific threats that continue to directly impact organizations today and offer suggestions for preventative actions that business executives can take to improve their overall security posture.



Note: Size of circle estimates relative impact of breach in terms of cost to business.
Source: IBM X-Force Research and Development.

Figure 1: **2011 Sampling of security incidents by attack type, monthly and impact.**

Emerging security issues

Traditional attacks are becoming more sophisticated

Many of the traditional security threats that have been prevalent over the last several years are continuing to evolve and spread. Several of the most noteworthy incidents, including attacks by organizations such as Anonymous and LulzSec, involved the use of "SQL injection," a technique first popularized in the 1990's.[3]

Such attacks target vulnerable databases to bypass authentication, access the private contents of the database and even compromise the operating system that hosts the database. Although many organizations have secured the primary web-based applications that provide access to these databases, updates and revisions to these systems and their supporting databases are often not subjected to review with the same level of rigor.

Another form of attack that has evolved is the use of "phishing," where attackers trick individuals into revealing personal information such as bank accounts, identification numbers and the like. In the past, phishers directed individuals to websites with names that were similar to established companies, deceiving them into revealing their private information.

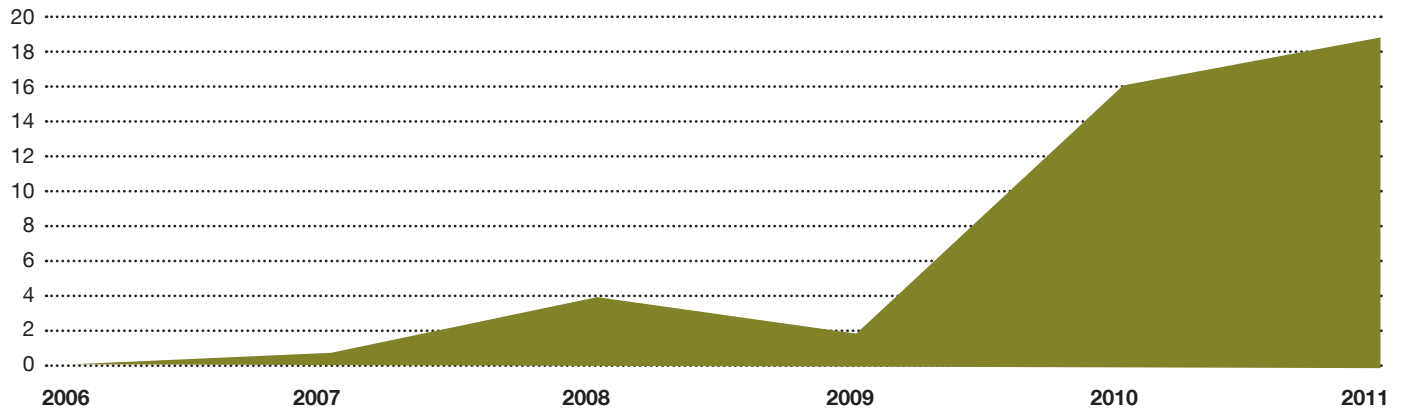
Today, phishers are directly attacking legitimate web pages and inserting dangerous sub-domain pages there. This further adds to the perceived legitimacy of the information requests, making access by unsuspecting users even more likely. Phishing attackers are also leveraging publicly available information from social networking sites to compose personalized messages for their potential victims, a targeted style of attack often referred to as "spear phishing."

An increasingly common technique is the mimicking of legitimate applications by programs with damaging consequences. One particular form of malware, MacDefender, disguises itself as a legitimate antivirus program. Once installed, it pretends to scan the computer, flagging random files as malicious to make it appear that the system is heavily infected. The malware then offers to remove the identified files for a license fee. If users select this option, they then have to register on a website, where credit card information is collected and charged. Other intrusions, such as Flashback, pretend to mimic legitimate programs like Adobe Flash; when downloaded, they inject unauthorized code into applications and direct users to access unintended websites. A recent study suggested that over half a million Mac users have been infected with variants of this Flashback virus.[4]

Taking more than your device to work

The proliferation of mobile devices has clearly had an effect on organizations over the past year. Not only are organizations looking to develop mobile strategies that address the needs of customers, they are adopting new policies for employees as well. As individuals look to leverage the power of a new generation of tablets and smartphones, the use of personal devices in the corporate environment will rise.

While the trend toward "Bring Your Own Device" can provide a host of advantages to end users, the lack of corporate ownership and control adds to the security challenges that organizations must address. The 2011 X-Force report highlights a clear uptick in the malicious activity targeting these mobile devices (see Figure 2).



Source: IBM X-Force Research and Development.

Figure 2: **Mobile operating system exploits, 2006-2011.**

Mobile devices provide an additional level of risk for a host of reasons. Because of the relationship between phone end users, telecommunications companies and mobile operating systems vendors, vulnerabilities can remain undetected for extended periods of time. This provides a larger window of opportunity for attackers.

Further, the growing number of mobile platforms and the impact of regulatory requirements exacerbate the situation. The availability of programs that enable "jailbreaking" – that is, installing unapproved third-party applications on a device – has made it easier for unauthorized individuals to obtain access to data on phones. Finally, mobile devices, which often combine GPS hardware with voice, messaging and data services, can be at risk for attacks that can monitor multiple aspects of a user's private communication – including recording location, messages, emails and phone calls.

Attack activity associated with mobile platforms has been relatively small compared to the volume of activity targeting traditional workstations. But in the future, we expect to see more security issues arising from mobile device adoption that keeps growing rapidly.

Risks of social media: Are we trusting without verifying?

Over the last several years, social media has transformed from a fringe activity into the number one online activity in the world. By the end of 2011, approximately 80 percent of the global online user population (over one billion people) was using social media.[5] This rapid growth provides a fresh breeding ground for fraud and scams that were once successful on email are now revitalized in this new environment.

Social media also adds another risk dimension: the amount of private information that users are pouring into social networks has shifted and simplified the paradigm of social intelligence collection, providing more complete pictures of individuals and networks that can be subjected to attacks. Individuals who are associated with an organization targeted by hackers may find themselves interacting with compromised accounts within their social networks, inadvertently exposing information or accessing sites which then infect them with malware. This can ultimately result in the theft or destruction of corporate data assets. Personal information can be targeted in an attempt to gain access to passwords, locate sensitive documentation and even disseminate malicious files throughout an organization.

Security in today's evolving world

Mobility, social media and web commerce are clearly entrenched concepts that are reinventing how organizations compete in today's business environment. Although these activities, by definition, engender some form of risk, it is far more realistic for companies to mitigate these risks than to attempt to avoid this new generation of technologies altogether. Based on IBM experience working with organizations, we see four opportunities for business executives to address these emerging security issues:

- Building a proactive security intelligence capability
- Developing a unified view of all endpoints, including mobile devices
- Protecting information assets at the database level
- Staying safe while staying social.

Emerging security issues for organizations: Attacks are becoming more sophisticated; mobile devices are increasingly being targeted; and social media is a fresh breeding ground for fraud.

Building a proactive security intelligence capability

In the past few years, the increase in attacks, the expansion of computing devices, and the explosion of data have created significant challenges for security practitioners. Even determining that a breach has taken place can be difficult, perhaps leaving organizations unaware of an exposure for months. While companies often have the raw data, they frequently lack the visibility and analytics to detect a problem. The 2011 Verizon Data Breach Investigations Report concluded that in 69 percent of breaches, good evidence of the breach existed in the organization's log files, but it was rarely found because of the number of data sources and a poor level of integration.[6]

Threat detection today therefore hinges on two elements: identifying suspicious activity among billions of data points, and refining a large set of suspicious incidents down to a manageable view of those that truly matter. This necessitates the use of real-time analytics across a spectrum of security operations. For example, by analyzing flows of data packets and monitoring user activities for anomalies, organizations can help to identify patterns that indicate potential insider data theft or compromise by external parties.

This advanced form of performing meaningful analytics across multiple data sources is referred to as security intelligence. It differs from traditional security measures in four ways:

- *The use of flow analytics* – In the past, logs from devices, applications, servers and infrastructure services provided a rear-view perspective of what activity was occurring across the organization. Today, advanced analytics can deliver current, real-time insights into user behavior, social media usage, mobile activity, cloud activity and more.
- *Predictive analytics and pre-exploit awareness* – Better understanding of misconfigured devices and unpatched vulnerabilities allow an organization to identify, prioritize and systematically address risks prior to an exploit.
- *Anomaly detection* – Traditional security efforts have focused on protecting the organization from known threats, such as publicly disclosed vulnerabilities and common malware. Today, advanced attackers develop targeted exploits for as yet undisclosed weaknesses, called "zero-day attacks," and so security teams also need to focus on activities and behaviors beyond those that are expected or pre-defined.
- *Easy to deploy and staff* – To capitalize on emerging security intelligence insights, security teams rely on dashboards and other forms of data visualization to make it easier to integrate various data sources and make it easier to spot threats.

Developing a unified view of all endpoints, including mobile devices

Given the proliferation and disparity of personal devices, and the trend toward using these devices in the work environment, the ability to manage them in a more holistic manner has become increasingly critical.

For many organizations, different security platforms are used to manage different categories of devices (for example, smartphones, laptops or tablets). While it is certainly possible to try to tie together disparate management systems into a single enterprise risk console, this is far easier and more likely to succeed if supported by a single underlying framework. It is also far easier to analyze and respond to security threats when data is integrated within a single platform. Well-defined and controlled security policies enable consistent management across endpoints, as do the selection of appropriate technologies and oversight of the entire enterprise security landscape.

Protecting information assets at the database level

While the increasing number of personal devices and end-user systems require time and attention, database servers still remain a primary target for breaches. While multiple systems are ordinarily breached in the course of an attack, it is important to remember that often the ultimate target is the valuable intellectual property, personally identifiable information, credit card data, and the like that the organization holds.

For companies to manage this risk effectively, they need to examine three primary issues: data location, business controls and regulatory compliance.

First, the organization needs to identify the locations of critical data and how they are maintained and categorized internally. Do they exist in a secure environment where physical and networked access is closely monitored, or are they located on an unknown server or even a physical file system that can easily be breached?

Second, has the organization established effective business controls, policies, architectures, processes and technologies that protect, monitor and audit access and use of this data by appropriate individuals? Does this protection still allow easy access for legitimate business purposes?

Third, in business environments where regulation exists with the goal of ensuring the security of personal information, is the organization able to demonstrate its compliance with these rules? Does it maintain the flexibility to adapt to ongoing regulatory changes?

Creating safer social habits

A September 2011 Ponemon Institute study indicated that only 35 percent of respondents had a written social media policy in place; and only 35 percent of that subset actively enforced the policy.[7] Unfortunately, there is no software or suite of end-point security products that can be easily deployed to defend against the many types and approaches to social engineering. As with most threats aimed at human beings, the best way to manage such risks is through policy and education.

Responsibilities that end-users should take, especially if they are engaging in social media using work-related devices, include:

- *Enable security and privacy settings.* It is important that end users understand what security and privacy controls are available in the social media sites they use regularly, even if they do not consider themselves to be active users. To decrease exposure to spam, scams and opportunistic attackers, their security and privacy controls should be set to maximum levels.
- *Friend only friends.* Social engineering attacks would not be so successful if they were not clever in some respects. Just as with real-world con artists, social media attackers begin their attacks by attempting to gain a certain level of trust from their targets. Faking a tangential work-related relationship via Linkedin, for example, lends almost instant credibility for the attacker. End users should consider friendship requests carefully, accepting those based on prior real-world relationships or provable connections. Users should also be made aware of the downstream impacts of their associations. Others who trust an individual may well assume that they can trust anyone who has established a connection with that same person.

- *Use caution with links and downloads.* Links and downloads have been a favorite vehicle for attackers to deliver malware to their targets since email became ubiquitous in the late 1990s. The trend has now evolved and expanded into social media forums. End users must exercise extreme caution, and carefully consider the source and appropriateness or relevance before they click on any links or download anything (particularly executable files). Trusted social media contacts can themselves have been compromised, so a skeptical eye toward any interaction with third-party content is a must.
- *Be wary of contests, gifts, prizes and special offers.* Prizes and other special offer scams also date back to the early days of email but continue to perform strongly in social media forms. Scammers typically use this type of offer to direct end users to a dead-end website that will load cookies or even spyware, or more often, to fake websites that mimic legitimate businesses or brands. Either way, the scammer is collecting personal information from its targets.
- *Remain cautious about disclosing work-related information.* End users should always consult their employers' appropriate use policies for social media when communicating information about the organization, colleagues, clients, products, services and projects they are currently involved in. In the absence of a written corporate policy, common sense may be the best guide in terms of posting work-related information. Posts should be considered carefully as they go public instantly and are essentially irretrievable.

Mobility, social media and web commerce are clearly entrenched concepts that are reinventing how organizations compete in today's business environment, and managing them more holistically has become important.

Seeing the complete picture

The 2011 X-Force report highlights the importance of taking a holistic approach to cybersecurity that addresses both business challenges and technical issues. For the busy executive, security is not an issue that can simply be delegated; it must be embraced as another important component of any plan for doing business in an increasingly complex and technology-driven world.

As mobile and social capabilities continue to multiply, so will the need for a unified approach to predicting, identifying and preventing attacks on individuals as well as the organizations they represent. Addressing the needs for predictive analytics, unified endpoint management, data protection and social guidance can help organizations manage the potential downsides of cyber risks.

To learn more about this IBM Institute for Business Value study, please contact us at ibv@us.ibm.com. For a full catalog of our research, visit

ibm.com/iibv.

Be among the first to receive the latest insights from the IBM Institute for Business Value. Subscribe to IdeaWatch, our monthly e-newsletter featuring executive reports that offer strategic insights and recommendations based on IBV research at

ibm.com/gbs/ideawatch/subscribe.

Access IBM Institute for Business Value executive reports on your tablet by downloading the free "IBM IBV" app for iPad or Android from your app store.

Authors

Jack Danahy is the Director for Advanced Security, IBM Security Systems Division, and is an international speaker and writer on topics of software, system, and data security. He is the founder and CEO of two successful security software companies: Ounce Labs, sold to IBM in July 2009, and Qiave Technologies, sold to Watchguard Technologies in 2000. He holds five patents in a variety of security technologies, including secure distributed computing, software analysis and secure system management. He is a distinguished fellow in the highly respected Ponemon Institute and has contributed to the development of legislation on computer security in both the U.S. House of Representatives and U.S. Senate. He can be reached at *jack.danahy@us.ibm.com*.

John Lainhart is the IBM Global Business Services' Global Security & Privacy Service Area Leader and U.S. Public Sector Cybersecurity & Privacy Service Area Leader. He represents IBM on the American Institute of Certified Public Accountant's (AICPA) Assurance Services Executive Committee's Data Integrity Task Force; and Strategic Advisory Council for the Center for Internet Security. He has held numerous positions in the Information Systems Audit and Control Association/IT Governance Institute, including International President and currently is a member of the Framework Committee and serves as Chair of the CobiT® 5 Task Force and Principal Volunteer Advisor for IT Governance, CobiT®, ValIT® and RiskIT® related initiatives. He can be reached at *john.w.lainhart@us.ibm.com*.

Eric Lesser is the Research Director and North American Leader of the IBM Institute for Business Value, where he oversees the fact-based research IBM undertakes to develop its thought leadership. Previously, he led IBM Global Business Services' Human Capital Management research and thought leadership development. His research and consulting has focused on a variety of issues, including workforce and talent management, knowledge management, collaboration and social networking, and the changing role of the HR organization. He can be contacted at *elesser@us.ibm.com*.

The authors would also like to acknowledge the ongoing work and contribution from the IBM X-Force team, including Jason Kravitz, Tom Cross, Leslie Horacek, Ralf Iffert, Paul Sabanal, Scott Moore, David Merriell, Mike Montecillo, Michael Applebaum and Kimberly Madia who prepared the content in the 2011 IBM X-Force Trend and Risk report referenced in this paper.

The IBM X-Force research and development team provides the foundation for a preemptive approach to Internet security. IBM X-Force is one of the best-known commercial security research groups in the world. For more information, visit **ibm.com**/security/xforce.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment. Through our integrated approach to business design and execution, we help turn strategies into action. And with expertise in 17 industries and global capabilities that span 170 countries, we can help clients anticipate change and profit from new opportunities.

References

1 "Leading Through Connections: Insights from the Global Chief Executive Officer Study." IBM Institute for Business Value. May 2012. www.ibm.com/ceostudy2012

2 This executive report is based on data collected in the 2011 IBM X-Force Trend & Risk report. Register to download the latest version at https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report

3 The Open Web Applicaation Security Project. "SQL Injection." December 6, 2011. www.owasp.org/index.php/SQL_Injection

4 Perlroth, Nicole. "Widespread Virus Proves Macs Are No Longer Safe From Hackers." Bits. *The New York Times*. April 6, 2012.http://bits.blogs.nytimes.com/2012/04/06/widespread-computer-virus-indicates-mac-users-no-longer-safe/?scp=1&sq=macdefender.com&st=cse

5 Press release. "It's a Social World Report: Social Networking Leads as Top Online Activity Globally, Accounting for 1 in Every 5 Online Minutes." comScore. December 21, 2011. www.comscore.com/Press_Events/Press_Releases/2011/12/Social_Networking_Leads_as_Top_Online_Activity_Globally

6 Verizon. "The 2011 Data Breach Investigations Report: A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Dutch High Tech Crime Unit." 2011. www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

7 Ponemon Institute. "Global Survey on Social Media Risks." September 2011. www.websense.com/content/ponemon-institute-research-report-2012.aspx

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
June 2012

Please Recycle

GBE03502-USEN-01