Kroll®

2012 Cyber Security Forecast

Top Ten Trends for the Year Ahead

» Table of Trends

0100000101101100011011000010000001101111011100100110011101100001011011100110100101111010011000010111010001101001011011110110111001110011001000000110011001100001011000110110010 10

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» "The events of 2011 suggest that the cyber security landscape will find public and private organizations are still on unsteady footing."

Karen Schuler, Practice Leader
Kroll Cyber Security & Information Assurance

Preface

›› 2012: What to expect and how to deal with it

010000001011011000110110000100000011011110111001001100111011000010110111001101001011110100110000101110100011010010110111101101110011100110010000001100110011000010110001101100101010

If there's one thing we learned from 2011, it's that no one is exempt from attack.

Some of the largest data breaches in recent history made news last year, sparking data breach dialogue around the world. Quite possibly the largest data breach ever ignited fears of widespread spear phishing. Advanced Persistent Threat attacks penetrated a respected security organization. And social causes fueled a new wave of hacktivism that affected millions of individuals. All in all, if not the Year of the Data Breach, 2011 was certainly the Year of Data Breach Headlines.

So how do you transform large-scale lessons learned into best practices for 2012?

We believe that effectively navigating risk starts with a firm awareness of the lay of the cyber security landscape. And that's where these trends come in. From mobile device security and cloud services to geolocation technology and international breach laws, you'll find the top ten areas to keep on your cyber security radar as you set out to mitigate risk in 2012.

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» A recent survey of IT professionals revealed that 73 percent of enterprises were allowing non-IT managed devices to access corporate resources.

iPass Inc. The iPass 2011 Mobile Enterprise Report.
September 29, 2011

» Mobile technology security threats will be at an all-time high.

0100000101101100011011000010000001101111011100100110011101100001011011100110100101111010011000010111010001101001011011110110111001110011001000000110011001100001011000110110010101 0

Mobile technologies are changing so rapidly that in some organizations the demand and pressure to deploy new technologies (e.g., tablet computers) will outstrip the organization's existing capabilities to secure them. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

Further Reading

Mobile Device Security: How to Protect Yourself and Your Data

Paying the Price for Those Free Apps

Say "Breach"

Digital cameras used by medical facilities to document patient treatment are becoming increasingly attractive to potential thieves. This type of data loss represents a potential HIPAA privacy law violation and could have serious ramifications for the healthcare industry.

But the use of digital cameras to violate data security policies isn't limited to healthcare. A recent case involved a non-profit worker who photographed donor checks and sold the account information to gang members as part of an ID theft ring.

Digital Download

Tips for Securing Your Mobile Workforce »

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» How does the next-generation workforce rate company IT policies on social media and device usage? Four out of five young workers consider them outdated—if such a policy even exists at all.

2011 Cisco Connected World Technology Report

» Social media will increase in popularity as a conduit for social engineering attacks.

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2012, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. Thieves will utilize clever tactics to coerce end-users into disclosing sensitive information, downloading malware, or both. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring, and log file analysis.

Further Reading

Social Media Makes Way for Social Engineering

Thought Leadership Series

Social Media in the Workplace

Considering the potential risks social media use can pose to organizations, businesses must give employees a clear set of guidelines on how to engage in social media safely and smartly. Discover the top three areas you should consider when developing your organization's social media policy if you want to transform your employees into data security ambassadors.

Combat Data Security Risks with Formal Guidelines for Employees »

It's no question social media poses real risks to your organization's data security. But, does this mean you should ban access to these sites company-wide? Find out what role social media has played in a few real-world security breaches and why striking a balance between the benefits and risks of social media could be the best approach for your business.

Examples of the Data Security Threats Within »

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» A recent study found that 40% of small businesses do not have a contingency plan outlining procedures for responding and reporting a data breach or loss.

National Cyber Security Alliance, Symantec, and Zogby International.
2011 NCSA / Symantec Small Business Study. October 2011.

» Small and medium-sized businesses (SMBs) will enter the crosshairs

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

"Hacktivism" may make headlines, but the fact of the matter is that data thieves are simply looking for the path of least resistance. Of late, that path has been leading directly to SMBs that house large amounts of valuable data but lack the data security budgets of their big business peers. Common modes of attack include everything from social engineering to SQL injection. In addition, ongoing use of legacy systems—weakened by postponed or overlooked upgrades and replacements—put SMBs at heightened risk.

Further Reading

Top Ten Security Mistakes SMBs Make

A Case for Consideration

Kroll worked with a small business with approximately 20 employees on staff—yet the company managed benefits administration for large corporations that employed thousands of people. As a result, the organization had amassed a very critical amount of data. When a break-in led to the loss of several laptops, the personal data of nearly half a million individuals was lost in the process.

Bottom line: It's dangerous to assume that a small organization carries less risk for breach—let alone a large breach of data.

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» According to 74% of IT and compliance officers surveyed, cloud providers have already been—or are very likely to be—selected without vetting their security practice.

Ponemon Institute. The Security of Cloud Infrastructure. November 2011.

» As cloud services gain in popularity, related breach incidents will flourish.

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

If we were meteorologists, we'd definitely be calling for overcast with a chance of storms. Companies are smartly embracing the cloud for the associated cost savings and ease of use. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

Further Reading

The NIST Definition of Cloud Computing

A Case for Consideration

Beyond privacy and data security issues, cloud computing presents concerns related to intellectual property protection and electronic discovery, as well. For example, we've seen a case where a foreign cloud provider refused to supply the data demanded by the court. The fact that the provider was outside the jurisdiction of U.S. courts didn't matter to the court—the organization chose the vendor and was required to take responsibility for their discovery obligations.

Bottom line: Think about all of the potential issues BEFORE contracting for cloud services.

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» "Gone are the days when cyber security is the sole preserve of specialists. Protecting sensitive information impacts our society from Main Street to Middle America—from people shopping in a store downtown or on the web, to the doctor utilizing digital devices to diagnose a patient, or to the collaboration occurring with an overseas colleague on a research and development project. We must all work together, in both the public and the private sector, to ensure that our computers and networks are secure against cyber threats."

Howard A. Schmidt, Cybersecurity Coordinator and Special Assistant to the President,
"A Dynamic Approach to Federal Cybersecurity," The White House Blog

» Business and government cooperation will be mission-critical for economic and infrastructure health.

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

Cyber crime has the capacity to cripple almost every aspect of commerce from the largest corporation to the individual consumer. Similarly, the security of U.S. infrastructure is being called into question in disturbingly real ways. For these reasons there is a growing sentiment among both private organizations and the U.S. government about the increased need for information sharing. Improved communication between the private and public sectors will not only give government the ammunition needed to take down major threats, it will also increase private entities' capacity to respond to large threats more effectively.

Joint Effort Brings Success

Operation Ghost Click—the FBI's two-year investigation of a global internet fraud ring that infected more than four million computers in a scheme to defraud the internet advertising industry—resulted in the arrest of six Estonian nationals this past November. Find out why collaboration was so important and what it could mean in the long run.

Operation Ghost Click Brings Down International Cyber Crime Ring »

Further Reading

Cybersecurity | The White House

Recommendations of the House Republican Cybersecurity Task Force

The Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PrECISE) Act of 2011

NIST Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» “I believe that consumers have a fundamental right to know what data is being collected about them. I also believe that they have a right to decide whether they want to share that information, and with whom they want to share it and when.”

Remarks by Senator Al Franken (D-MN) at a hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law: Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy Opening Statement

» Privacy concerns will keep geolocation technology in a white-hot spotlight.

01000001011011000110110000100000011011110111001001100111011000010110111001101001011110100110000101110100011010010110111101101110011100110010000001100110011000010110001101100101 0

Geolocation technology is the quintessential double-edged sword. On one hand, consumers love the convenience of innovative mobile apps and services utilizing this technology. On the other, the backlash against surreptitious tracking or disclosure can be swift and strong. In fact, several federal bills were introduced in 2011 dealing specifically with the protection of geolocation information. It seems unlikely any will become law in 2012, but we can expect to see privacy advocates urging businesses to adopt an opt-in or consumer consent model.

Further Reading

When it comes to new technologies, failure to anticipate privacy issues can have significant consequences

Legislative Lookout

Geolocation Privacy and Surveillance ("GPS") Act »

Sponsors: Senator Ron Wyden (D-Ore.) and U.S. Representative Jason Chaffetz (R-Utah)

Goal: To establish a uniform standard for government access to geolocation data and clarify how much evidence prosecutors and law enforcement officers need to remotely track individuals' movements, as well as when private companies can respond to legitimate law enforcement requests and what obligations they have to protect their customers' information.

Location Privacy Protection Act »

Sponsors: Senator Al Franken (D-MN) and Senator Richard Blumenthal (D-CT)

Goal: To close current loopholes in federal law to require any company to obtain customer consent before obtaining location data from the customer's smartphone or other mobile device and sharing the customer's location data with third parties.

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» Cyber security incidents can often be detected through log analysis: 64% of healthcare organizations surveyed said critical events are reported in their audit logs.

Healthcare Information & Management Systems Society. 4th Annual HIMSS Security Survey. November 2011.

» Management and analysis of logs will gain more respect for its role in incident preparedness and response.

Security incidents have increased in sophistication and frequency in recent years and one of the most effective modes of response involves maintaining complete logging for the network and key applications. While historically undervalued, logging provides vital information that can be utilized for analysis of network activities and documentation of security incidents. As companies begin to see the error in their ways in 2012, they will begin to implement formal risk assessments to look for security weak spots.

Further Reading

Advanced Threats Touch Two-Thirds Of Enterprises

Digital Download

The Advanced Persistent Threat, or APT—we've all heard the term, but what does this really mean and, more importantly, how big is the threat to organizations across the country, large and small? We sat down with Alan Brill, CISSP, CFE, DFCA, a senior managing director with the Cyber Security & Information Assurance practice of Kroll, to get some answers to these and other questions on the topic.

Advanced Persistent Threats and the Evolution of Cyber Crime »

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» In 2010, organizations that engaged external consulting support to manage a data breach reduced per-record cost by 11%.

Ponemon Institute. 2010 Annual Study: U.S. Cost of a Data Breach.
March 2011.

Incident response teams will get a permanent seat at the table when it comes to standard business operations.

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

Historically, incident response teams were made of employees from across the organization tapped to mobilize only if and when security incidents occurred. But to remain competitive in today's market companies need to upgrade incident response teams from contingency plan status to day-to-day operations. Effective incident response teams can include a group of full-time employees designated as incident responders or a team of outside consultants (via a third party) hired for 24/7 incident response support.

Further Reading

Download Kroll's expanded list to find out why these 10 questions are so important.

Top 10 Data Breach Questions

- Was personal data compromised from your systems?
- Did a data breach really occur?
- Is the intrusion or data breach still occurring?
- Have you created a defensible and diligent plan to remediate the intrusion?
- Was the data breach accidental or malicious?
- Have you alerted outside counsel?
- Do you understand your legal obligation for breach notification?
- How effective is your crisis communications plan?
- Was your data breach response plan effective in responding to this incident?
- How can we avoid a data breach in the future?

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

» In a recent survey of IT and IT security practitioners, regulatory compliance (50%) and response to a data breach incident (46%) took top billing as main drivers for data breach protection programs.

Ponemon Institute. Best Practices in Data Protection. October 2011.

» Companies will overlook key vulnerabilities, as regulatory compliance continues to drive organizational security.

0100000101101100011011000010000001101111011100100110011101100001011011100110100101111010011000010111010001101001011011110110111001110011001000000110011001100001011000110110010110

Let's face it—state and federal regulations remain the yardstick by which the comprehensiveness of data privacy and security are measured. But using such a "checklist mentality" to drive security initiatives is dangerous because a number of data security regulations overlook basic IT security controls. Certainly there are regulations that address the need for encryption or the development of an incident response plan but few require a wide range of best-practice controls such as up-to-date anti-virus software. As more breaches occur as a result of security gaps, we should expect to see governing agencies offer specific guidance on risk assessment and standard IT security controls.

Further Reading

Impact of SEC Cyber Security Disclosure Guidance

Digital Download

Use this handy guide to help evaluate the measures you—and your third-party business partners—have in place to minimize your organization's data loss potential.

The Secret Six of Data Security »

Download this resource for insight into common questions surrounding the data security requirements outlined in Massachusetts 201 CMR 17.00.

Legislative Updates FAQ:
Massachusetts 201 CMR 17.00 »

0001011101000110100101101111011011100111001100100000011001100110000101100011011001010

> »“Although the basic principles and objectives of the 1995 Directive remain valid, these rules are not adapted to some new and emerging technologies and applications like social networks. We need to maintain both objectives of the original Directive, to ensure the free movement of personal data across the territory of the Union and to ensure a level of data protection. In a world of ever-increasing connectivity, our fundamental right to data protection is being seriously tested.”

Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner
“Building trust in the Digital Single Market: Reforming the EU’s data protection rules,”
November 28, 2011

» Breach notification laws will gain traction outside of the United States.

0100000101101100011011000010000001101111011100100110011101100001011011100110100101111010011000010111010001101001011011110110111001110011001000000110011001100001011000110110010101010

While the U.S. Congress struggles to reach consensus on a federal breach notification law, internationally the idea is gaining momentum. Companies with a global presence should watch these developments closely because they could have a significant impact on their operations abroad.

Further Reading

EC Releases Final Draft of EU Data Protection Reforms

Proposed Canadian Breach Notice Requirements

Legislative Lookout

- In January 2012, the European Commission released its final draft of the EU Data Protection Directive » (95/46/EC) to require breach notification to individuals and Data Protection Authorities. If approved, this would expand notice requirements to industries beyond just telecoms and ISPs.
- Germany already started requiring breach notice in all sectors in 2010.
- The Netherlands is considering requiring all sector breach notice requirements as part of its revision of the Dutch Data Protection Act ».
- Canada is considering mandatory breach notice as part of proposed revisions to PIPEDA », which governs how Canadian businesses collect, use, and disclose personal information.
- The UK Information Commissioner's Office » issued guidance saying they "expect" notice of "serious" breaches.
- The Ireland Commissioner issued guidance » that they "recommend" notice of all breaches.

» Epilogue

010000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

STAY CONNECTED

Join us as we continue the conversation throughout 2012.

Subscribe » to our e-newsletter and get an in-depth look at a different trend each month.

Visit our blog, A Dialogue on Data Security », for weekly insights from our team of cyber security experts.

CONTACT US

Phone: 1.866.419.2052

Email: information@kroll.com »

Web: www.krollcybersecurity.com »

About Us

0100000010110110001101100001000000110111101110010011001110110000101101110011010010111101001100001011101000110100101101111011011100111001100100000011001100110000101100011011001010

An Integrated Global Approach

At Kroll, we've spent nearly 40 years helping many of the largest organizations around the globe reduce their risk. Our worldwide multidisciplinary teams provide a suite of investigative and technology services to identify, manage, and respond to data security risks and to assist with complex investigation or litigation matters involving electronic evidence.

Kroll Cyber Security & Information Assurance provides scalable solutions that span the full information security and incident response spectrum, including:

- Data Security & Privacy
- Risk & Vulnerability Assessments
- Computer Forensics
- Incident & Data Breach Response
- Data Analytics