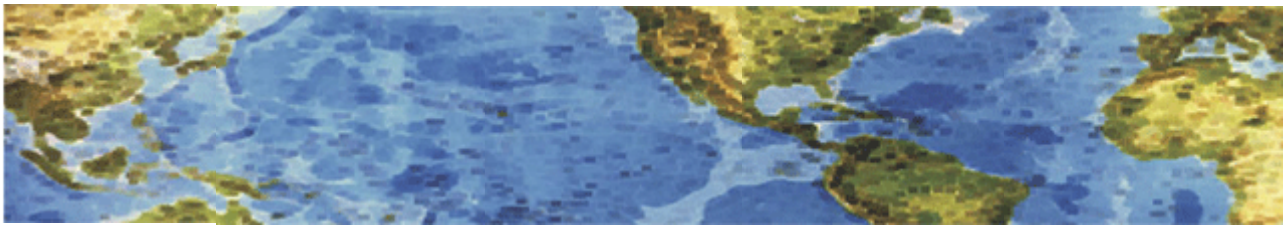
HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 December 2013 Newsletter

With each new year, comes a new round of cybersecurity risks – and most of the old ones are still risks also.

What we are doing is not working. We need to review what we are doing and why. We need to re-evaluate everything, from passwords to pentests to firewalls to DLP. We have to stop doing the same thing over and over again and expecting different results each time. Companies and individuals need to start looking for alternative security technologies to augment or outright replace many of the technologies and policies that have failed time and time again. To help businesses and individuals prepare for the year ahead with appropriate risk mitigation and response solutions several companies and security individuals have identified cybersecurity trends that indicate a changing tide in cyber standards. Responding appropriately to these trends will require all size organizations and individuals to take stronger actions and safeguards to protect against reputational, financial and legal cybersecurity risks.

The new cybersecurity issues for 2014 will include:

National Institute of Standards and Technology (NIST) and similar security frameworks will become the de facto standards of best practices for all companies: Cybersecurity strategies largely designed for companies that were part of the "critical infrastructure" will become more of an expectation for everyone, from conducting an effective risk assessment to implementing sound cybersecurity practices and platforms. Organizations that don't follow suit may find themselves subject to lawsuits by individuals and companies, actions by regulators and other legal repercussions.

As new laws are passed that reflect the NIST guidelines and look more like the EU privacy directive, all size U.S. companies will find themselves ill-prepared to effectively respond to the regulations, if they even know them. To minimize your risk, companies will have to get smart on these standards and make strategic business decisions that give clients and customers confidence that their information is protected.

The data supply chain will pose continuing challenges to even the most sophisticated companies: It is not unusual for companies to store or process the data they collect by using third parties. However, the security that these third parties use to safeguard their client's data is frequently not understood by companies that hire them until there is a breach. Companies need to vet their subcontractors closely and get specific as to the technical and legal roles and responsibilities of these subcontractors in the event of a breach. This requires technical, procedural and legal reviews.

The malicious insider remains a serious threat, but will become more visible: Information technology has simply made the insider's job easier. In 2014, a significant number, almost half, of data breaches will come at the hands of people on the inside. However, as the federal government and individual states add muscle to privacy breach notification laws and enforcement regimes, these hidden insider attacks will become more widely known. Thwarting an insider threat requires collaboration by general counsel, information security and human resources.

HALL ASSOCIATES

Corporate boards (and individual CEOs) need to take a greater interest in cybersecurity risks and the organization's plans for addressing them: With more and more data breaches covering more and more people- from theft of trade secrets to loss of customer information - in the headlines, management should focus on the connection between cybersecurity and an organization's/individual's financial well-being. For example, what are your strategic plans for protecting non-public information? Management also needs to look at risk-mitigation plans for responding to a possible breach. As corporate boards carry out their fiduciary responsibilities, they must also protect the company from possible shareholder lawsuits (and lawsuits and class action lawsuits for those caught up in the data breach) that allege the company's cybersecurity wasn't at a level that could be reasonably viewed to be 'commercially reasonable' and that incident response plans weren't in place to mitigate the risk. The challenge management faces is determining what is a reasonable level of security and response, and who should make that call. Is it their IT team, an industry expert, an independent third party?

Sophisticated tools will enable smart companies to quickly uncover data breach details and react faster: Management must realize that even the best firewalls and intrusion detection systems cannot stop all attacks. But technological progress that occurred over the last 12 months will enable companies to unravel events and see with near–real-time clarity what's happened to their data and how much damage has been done. Most organizations have invested in preventative security technologies, but remain unprepared to launch an effective response to a leak or intrusion. Without the right tools and policies in place beforehand, they find themselves suddenly under intense pressure to investigate, track and analyze events.

New standards related to breach remediation are gaining traction and will have a greater impact on corporate data breach response: Credit monitoring will no longer be the gold standard in breach remediation in 2014, as lawmakers, consumer advocates and the public at large continue to raise questions about the relevancy and thoroughness of this as a stand-alone solution. These parties will demand a more effective alternative. While no legal guidelines currently exist for consumer remediation, the FTC and states like California and Illinois are already offering guidance that suggests a risk-based approach to consumer remediation will be the way of the future.

As cloud and BYOD adoption continues to accelerate, implementing policies and managing technologies will require greater accountability: The development and evolution of cloud services and BYOD have moved at a whirlwind pace, leaving IT departments scrambling to get out in front of the technologies and employee usage. In 2014, IT leaders will need to work closely with senior leadership and legal counsel to adapt policies in a way that addresses changing legal risks, while effectively meeting the needs of the organization. Organizations must realize that even if they don't want to deal with this, they're not going to have much choice.

Expect to see a sharp increase in attacks against end-users and administrators who are accessing and controlling cloud-based services (both public and private clouds). Much of the focus is on the security of the cloud itself but very often the end-users are left to their own while connecting from less secure public networks. Administrators in particular will be targeted as they hold the keys to the cloud-based kingdom.

Expect to see large increases in attacks (i.e. Cryptolocker) against individuals and individual computers in networks. Once such ransomware gets into any computer, the entire network it may be attached to is at risk.

This will be the year for advancements in authentication. Even though good multi-factor authentication systems have existed for years, most organizations and individuals have relied on passwords to the exclusion of these other technologies despite clear demonstrations that usernames and passwords just aren't enough.

With the continued development and proliferation of intelligent portable electronic devices (smartphones, tablet computers, etc.), we will see a significant rise in account compromises resulting from the credentials for those accounts being stored on unsecured devices. While the user may have selected a password of sufficient length, when it's stored on an unsecured device it may be easily recoverable by an attacker.

The Internet of Devices will become security critical: Up to now, the internet connected mostly people. The end point of an internet connection was usually implemented using a PC, a server or more lately tablets and phone. But foremost, a person was operating and using the device connected to the network. In parallel to this "internet for people" we always had an "internet for devices": Small control systems and embedded devices that delivered metrics and control to other devices or larger control networks. Up to now, the proliferation of these devices was limited to specialized networks and environments. However, in particular the advent of IPv6, and the continuation of Moore's law to deliver cheaper and more powerful devices, will make it much easier to deploy devices ubiquitously. We already see a surge in internet controlled home automation and alarm systems. Cars with not one but several IP addresses, sub $50 "servers" as implemented in the Raspberry Pi project and projects like Androino to deliver sensory and control capabilities to the masses. These technologies frequently take advantage of cloud computing to supplement their limited computing capacity and heavily rely on commodity networks for data exchange. We have seen successful attacks against these devices by exploiting unsecured communication networks and will see an explosion in such attacks. Later on, complete takeover of the device by injecting exploit code into the insecure communication stream may be achieved.

The new HTML5 web specification has device geolocation baked in. With just a few lines of code, any website can now enable geolocation features, potentially leaving geo-artifacts on any device with a web browser. The recent US Supreme Court case, U.S. vs. Jones, demonstrates how interested law enforcement has been in geolocation monitoring. There will be a much wider range of investigators, both public and private, beginning to take advantage of geo-artifacts present on nearly every computer and mobile device, giving the ability to put the device at a particular place at a particular time.

Financial institutions will increasingly deploy mobile and cloud technologies and integrate their partners, suppliers and customers, so that their data perimeters are becoming much harder to define. As a result, they will have to essentially redefine the concept of a network perimeter. They should do this by developing a much more dynamic cyber security approach that includes customer training, outside connections cybersecurity audits, actionable threat intelligence, advanced adversary hunting as well as data protection and access controls developed at a much greater degree of granularity.

Can find additional information at the following:
http://www.businessnewsdaily.com/5563-7-cybersecurity-risks-for-2014.html
http://www.sans.edu/research/security-laboratory/article/2140
http://www.boozallen.com/media-center/press-releases/48399320/booz-allen-releases-annual-cyber-security-trends-for-2014