cyberSecure
PRODUCED BY ALM

December 15-16, 2015 | The Sheraton Times Square | NYC

Event Primer *Inside this issue:*

See page 8 for cyberSecure Event Details

ABCs for Cybersecurity Solutions the C-Suite Should Know

Jamie Sheller, The Legal Intelligencer

No business, no matter how sophisticated, is immune from a data breach or privacy incident and today's interconnected business ecosystem requires a shift from security that focuses mainly on prevention and controls to a broader risk-management response approach. Information security is not just a technical problem and the solution is not simply buying more software. As such, information security must involve balancing people, processes and technology to protect an organization's most valuable assets from the most relevant threats. Overseeing and monitoring this is the board's most important responsibility. Directors must be prepared to take an active role in understanding cybersecurity and privacy risk within the context of the corporation's overall strategy and operations.

It is incumbent on officers, directors and the management team to align their organization's cybersecurity enterprise management. An organization would be best served by engaging robust training and high-tech solutions to organize, explore and address critical areas. The following are key steps:

- **Appoint a committee.**

Appoint a board committee to focus on cybersecurity and privacy. (A separate enterprise risk-management committee is already required by Dodd-Frank for large financial institutions.)

- **Be proactive and discuss cyberrisk enterprise management.**

The board should be given access to adequate cybersecurity expertise and should regularly discuss current methods and approaches. Ensure the board is notified of all breaches (and possibly significant breach attempts). Make a commitment from the top down, both culturally and financially, to rigorously protect cybersecurity. Oversee the development of written policies and documentation to support the information security program.

- **Clearly identify all critical assets.**

Know the company's most valuable intellectual property and consumer-based informational assets, where they are located or stored, and how they are being protected (especially if they are housed and controlled by a third-party vendor or cloud service). Decide what warrants the most protection and how to protect each class of assets.

- **Data-breach response plan should be put in place.**

Make sure there is a robust data-breach response protocol in place that's well founded and repeatable. This includes escalation procedure, communication plan, incident response plan (depending on type of attack), a recovery plan and designated external breach coach lawyer for consultation to comply with legal notice requirements, regulatory enforcement and legal actions. Ensure your incident response plan (IRP) identifies key people within the organization that will drive the response. Ensure your IRP includes additional external "tiger team" experts often called upon in a data breach matter, such as a security breach lawyer, computer forensics, victim notification and public relations, for starters. A preset

See **SOLUTIONS** next page

7 Cyber Risk Stakeholders and Why They Matter

Thomas Reagan, Property Casualty 360°

Everyone—from individual employees to risk managers to your board of directors—now has a stake in managing cyber risk comprehensively, across the enterprise. Read on to learn about the seven key stakeholders other than the IT professionals to consider as you look at your cyber risk management strategy.

Risk manager: Risk managers can ensure various stakeholders are connected in terms of assessing, managing, and responding to cyber threats. They also have the best understanding of how the evolving cyber insurance market and overall risk finance options also is important. Even if they're not technology experts, they understand risk, so they're usually the best-positioned to coordinate cyber risk management across the company.

CEO/Board of Directors: The CEO and the company's board of directors may have a fiduciary duty to assess and manage cyber risk. Increasingly regulators, including both the Securities and Exchange Commission and the Federal Trade Commission, have made clear their expectation that top leadership to be engaged on the issue. And shareholders may be starting to demonstrate similar expectations.

CFO: From a financial perspective, concerns may range from the potential costs of a cyber event to the impact could be on the bottom line to the security of the company's sensitive financial information. CFOs should also critically evaluate the cost/benefits of growing investment in cyber security to drive the most efficient improvements to overall cyber risk profile.

Legal/Compliance: As regulations around cyber develop, legal and compliance roles become increasingly important to evaluate regulations and inform corporate policy. If a cyber incident occurs, lawsuits often follow within hours. Legal and compliance teams may help drive the appropriate breach response.

Operations: Key managers often are a first line of defense against cyber events. Should an event occur, they are critical to supporting the response and helping maintaining daily operations, business processes, and workplace stability.

Human Resources/Employees: The human element of cyber risk cannot be overlooked. Simple errors—or deliberate actions—by employees can lead to costly cyber incidents. Training on best practices is critical, especially with the rise in sophisticated "spear phishing" attacks targeting specific employees. And in an era of Bring-Your-Own-Device, employers should have a plan for dealing with personal devices used by employees who leave the company.

Customers/Suppliers: Interactions with customers and vendors can open you up to an attack. You need to understand the protections they have in place so they don't become the weak point in your cyber defenses. You should clarify in your contracts how to collectively respond to cyber events, as cyber risk can develop anywhere along the supply chain. Protecting your organization's data and individuals' privacy is becoming more difficult by the day. Successful cyber defense strategies are comprehensive and multi-pronged. A critical component requires understanding and defining the roles and responsibilities of all key stakeholders. ■

rapid engagement letter is also vital. (Note: If you have cyberliability insurance coverage, many insurers can give you access to their prevetted tiger teams.)

Make sure current reporting lines make sense given the responsibilities and accountability needed to execute the response plan. Make sure the right employees, possessing the appropriate skill sets, are adequately empowered. Anticipate and avoid any potential conflicts of interests, e.g., if the individual charged with overseeing cyberdefense is the same person who reports up the chain about breaches and oversees any response. Have a workflow plan with inside and outside counsel considering the legal ramifications of attorney-client and work-product privileges. Have a plan to deal and comply with competing interests such as FBI, U.S. Secret Service, local law enforcement, attorneys general, and other regulatory agencies when security incidents occur and build relationships with these entities for sharing and obtaining information about cybersecurity threats.

Identify data, networks or services that are critical to the organization's continued business and prioritize those items in the plan to ensure operational continuity during a crisis. Make sure there is an accurate and current network topology diagram that is updated and reassessed as internal and external factors change. Evaluate the effectiveness of the company's business continuity plan in the context of a cybersecurity incident and make sure it is updated. Make sure a breach response plan is current and that it is regularly updated. Run mock or tabletop exercises to test the plan's efficiency and efficacy.

- **Emphasize and ensure good IT hygiene.**

Make sure the company is recruiting and retaining IT security talent. Require internal audits to provide annual "health check" assessment reports, conducted by an independent source, that cover all domains of cybersecurity. Implement or ensure the use of robust access controls, data security controls and information-protection processes to help thwart the large majority of potential incidents. Take steps to stay current about the latest cybersecurity intrusions and software patches. The IT budget should adequately provide for cybersecurity needs, including a cybersecurity event.

- **Focus on detecting, monitoring and auditing.**

When the company loses key IT personnel, audit for known risks or red flags that might have contributed to their departure and have a succession plan to replace turnover and retain talent. Build a comprehensive database of security incidents that supports improvements.

Perfect security doesn't exist but an organization needs to learn and improve. Develop detection and continuous monitoring capabilities to address anomalies and threats to your company's assets. Timely detection increases a company's critical cyberresilience. Have a plan for regular cybersecurity assessments or penetration testing by independent third parties. Understand how peer organizations are being attacked, affected and defended.

- **Good third-party security management.**

Ensure an appropriate due diligence and vetting process for trusted third parties and cloud providers. Be aware of cyberliability risks associated with third-party outsourcing and ensure the board has a list of third-party relationships with appropriate liability agreements in place.

- **Harbor effective organizational communication.**

Make sure the organization has relationships with appropriate national and local authorities (FBI, etc.) and experts (a breach coach) for quick cybercrime response. Boards should meet with the chief information officer or chief information security officer and discuss strategy and current projects, including roadblocks like budget, lack of organizational participation and buy-in. There can be competing pressures that limit the IT department's ability to deliver security, so open communication with the highest level is needed.

Require management to communicate the enterprise risk-management organization's expectations and approach to cybersecurity. Understand what percent and total revenue in the IT budget or other budgets are being used for cybersecurity. Ensure the reporting chain between the CISO, CIO and CEO/COO meets best practices for optimal cybersecurity communication.

- **Instill good employee training.**

All employees should be trained and made aware of their role relative to cybersecurity, as cyberrisks are most often caused by human behavior rather than system flaws or technology weakness. Have ongoing cybersecurity training programs and develop a process to deal with policy violations and noncompliance.

- **Justify and know cyberrisk insurance coverage.**

The board should meet with the chief risk officer to ensure that cyberrisk coverage is sufficient for potential cyberrisks. Understanding the cost per record in data breaches and other statistics can inform judgment.

- **Keep reassessing.**

Periodically reassess your company's cybersecurity program through regular reviews, meetings with decision makers, experts and stakeholders. Find the right balance between innovation, business functionality and risk. ■

How Much Should Firms Pay to Protect Themselves From Hackers?

Nell Gluckman, The Am Law Daily

Whether it's to steal intellectual property, information on pending mergers or the credentials to bank accounts, cybersecurity consultants say that foreign governments and organized criminal groups are after the data stored inside many large law firms.

The American Bar Association estimates that 80 percent of the 100 largest firms in the U.S. have been breached, while a survey of members of the International Legal Technology Association released last week showed that for the first time ever, security management is viewed as the biggest challenge facing legal IT departments.

What should law firms be doing about this threat? Cybersecurity consultants spoke with The Am Law Daily about how the most cautious firms are protecting their clients' data from hackers and what they're spending.

Larry Ponemon, who runs his own research institute and consultancy on privacy and data protection, said there are four key people that firms with 500 lawyers or more should have on staff.

The first is a chief information security officer who oversees cybersecurity. This person should not report to a chief information officer, but to an executive body, Ponemon said. Security technology isn't going to yield the kind of return on investment CIOs are looking for, so they're likely to stop cybersecurity advocates in their tracks.

The second important staff member would be "someone who is a regulatory policy wonk," Ponemon said. This person should understand data protection laws in all the countries a law firm works in.

The third individual is a security architect who makes sure that the technology a law firm is using to protect itself is built properly and is working according to plan.

Finally, large law firms should have a forensics expert on staff who can figure out how to stop the bleeding when a breach occurs, said Ponemon. He added that the more ambitious firms will also have someone on staff who is involved in training lawyers and staff members to operate more cautiously when dealing with data, email and their portable devices.

> *'It's not uncommon for [the cost of a breach] to be in the millions, and it could be in the tens of millions.'*
>
> —Charles Carmakal
> Vice President, FireEye

"Law firms have a unique role in data protection," Ponemon said. "They have the ability to discover and collect as much information as they need to when trying a case."

He estimated that about 10 percent of major law firms have a well-defined security program that looks something like what he recommends. He added that those firms spend between $3 million and $5 million per year on cybersecurity.

Last week, Chase Cost Management released a survey that said spending on information security at Am Law 200 firms rarely exceeds 1.9 percent of gross revenue, as noted by sibling publication LegalTech News. Half the CIOs who responded to the CCM survey said they felt their

See **PROTECTION** page 5

Internet of Things Will Lead to Complex Legal Questions

The issue of risk management is 'potentially enormous' with the IoT and it will pop up in 'unexpected ways.'

Ed Silverstein, Legaltech News

The Internet of Things (IoT) – which adds connectivity to everyday devices – could create multiple and sometimes unexpected legal issues in the coming years.

There may be concerns arising on risk management, security, privacy, consumer protection and data use.

Despite these challenges, it is clear that many businesses and consumers will want to take part in the IoT economy. In a new study, Juniper Research has predicted that retailers will spend about $2.5 billion in hardware and installation to be part of the IoT revolution. Some popular products used to be part of the IoT include hardware such as Bluetooth beacons and radio frequency ID tags.

Compare that amount to the estimated $670 million that will be spent this year. On top of that, the number of items connected to the IoT is predicted to be 38.5 billion in 2020. One Cisco study has even placed the number of things connected to the IoT at about 50 billion by 2020.

"It's really starting to show up on people's radar screens," says Trey Hanbury, an attorney at Hogan Lovells, about the IoT.

Hanbury, who previously worked at the Federal Communications Commission and was director of government affairs for Sprint Nextel, said that, "People are becoming more cognizant of the risks."

He predicts that the issue of risk management is "potentially enormous" with the IoT and it will pop up in "unexpected ways."

That is in part due to the involvement of multiple parties, even if it involves something as simple as a kitchen appliance such as a coffee maker, because the product has to be enabled to be connected.

These parties include: device manufacturers, service providers for connectivity, application providers, as well as a host of traditional players, he said.

If something goes wrong with the coffee maker when involving the IoT, there is just not the potential blame on the manufacturer of the coffee maker, and potential allegations the manufacturer designed a faulty product. All of the parties potentially could be blamed in connection with the role they played.

The IoT leads to a "chain of responsibility" within the ecosystem, Hanbury said. Theories of causation and legal accountability will need to develop and evolve along with the technology, adds Alan Cohn, an attorney with Steptoe & Johnson.

It also may lead to a case-by-case analysis on where the risk of loss should be, he adds. "That's

going to be a real challenge," Hanbury said. He noted too it may not be clear how to assign liability in such situations.

So companies involved in the IoT are going to have to figure out how to manage the risk when taking part in the IoT economy, according to Hanbury. Those challenges will likely apply to every participant not just the smart device manufacturer.

The choices include trying to figure it out by including details in contracts or waiting until there is litigation and fighting it out in court – where class actions are a risk. Hanbury prefers taking the approach that "sooner the better" – so that means doing it earlier in the process on the "front end."

A related issue arises: Is a company going to need to void warranties if a user connects to a smart device? "You may need to think about it," Hanbury warns.

Also, typically, most products that comply with industry safety and tech standards do so voluntarily. What will these standards say about IoT uses?

Bruce Heiman, an attorney at K&L Gates who formerly was Legislative Director and Trade Counsel to Sen. Daniel Patrick Moynihan (D-NY), said that industries are involved in a half-dozen different efforts to set industry-led standards on IoT and machine-to-machine communications – that will help set baseline measures and best practices.

> *'There is great risk for lawsuits with pretty much anything new, especially where people aren't clear on exactly how something works.'*
>
> **— Alan Cohn**
> Steptoe & Johnson

In addition, there is the possibility that intelligence will be introduced into business procurement activities, Hanbury said. How about the case of a utility which finds the best prices for products? When two utilities communicate what happens if they agree to "collude"? Does that become an anti-trust violation?

There are "a whole host of issues" driven by collusive behavior or intent to reach an agreement, Hanbury explained. The questions lead to a "kind of grey area," Hanbury confirms. Questions will arise if companies should have known that the utilities would perform in a way that ends up creating antitrust concerns. That also means that regulators – such as the Department of Justice, the Federal Trade Commission and the Securities and Exchange Commission – all may need to review these issues, Hanbury said.

"We're going to need to figure it out, hopefully before it starts to take place," Hanbury said.

Privacy is another area where the IoT will lead to many issues. The IoT and machine-to-machine communications can lead to the creation of a lot of data. Data are collected on consumers and businesses. One example is finding out that drivers speed frequently or they take longer than other motorists to apply the brakes. Could that lead to higher auto insurance rates as companies leverage that data?

"The privacy implications are potentially huge," Hanbury said of the IoT ecosystem.

"Information can be put to both good and bad purposes," Heiman adds. For instance, it could be used to lower insurance rates or used in an attempt to get more flexibility from regulators, he said.

He confirms there will be more information created on companies, but Heiman does not see it as being qualitatively different from what is already out there – in terms of what can be brought up by regulators or opponents in litigation.

From the point of view of consumers, they will likely need to be informed how the data on them will be collected and for what purposes it will be used. Companies will need to think about if they really need to know personal information, such as what time someone makes coffee in the morning, Heiman said. Privacy rights of employees may create issues, too.

It is also noteworthy that with the IoT and machine-to-machine communications, sensors will communicate among each other. "The human element will be removed from practically all of this," Heiman said. That makes the need for guidelines for machines even more important.

Juniper Research further predicts that the IoT will lead to a security model to ensure there is a "robust" means of identifying network breaches. If suspicious activity is detected, parts of the network can be shut off to prevent spread of the cyber-attack, the firm says. Heiman says there could be far more points of possible cyber-attacks with the IoT so companies need to address related security concerns.

As for now, lawyers need to get ready for the IoT revolution and may face unanticipated questions on a host of issues.

"I don't know if we have all of the answers," Hanbury said about today's level of IoT preparedness.

"There is great risk for lawsuits with pretty much anything new, especially where people aren't clear on exactly how something works," Cohn said. "That said, common law has reliably—if slowly—adapted to technological advances, and the Internet of Things shouldn't be much different. ■

PROTECTION continued from page 3

firm wasn't spending enough.

But there are some steps that law firms can take that don't cost anything, said Charles Carmakal, a vice president in the forensics division at FireEye, the IT security company that raised $303.6 million in an initial public offering in 2013 and remains on the hunt for acquisitions in the cybersecurity space. (LegalTech News reports that Mandiant, a division of FireEye, has found that 80 of the 100 largest U.S. firms have been hacked since 2011.)

A mistake that Carmakal sees a lot of firms make is using the same administrative password across all their systems. Another common issue is that senior attorneys often will open any attachment they receive, he said.

"Every attorney wants new business, so if they get an email from a prospective client, there's no reason they wouldn't click on a link," Carmakal said. (A report released last month by Verizon showed that members of the company's in-house legal department were most likely to click on phishing emails and links.)

Carmakal said that taking steps to limit the level of access that employees have to their own systems, while unpopular at most firms because it slows down work flow, is another way to reduce risk that costs only time. He added that there are free programs available that will prevent unauthorized applications from running.

When law firms do experience a breach, they call people such as Carmakal to respond. The costs that ensue can dwarf those that would have prevented a breach, he said.

"It's not uncommon for it to be in the millions, and it could be in the tens of millions," said Carmakal about the costs incurred by clients seeking to deal with an incident. "It depends on the situation."

A handful of CIOs at Am Law 100 firms did not respond to interview requests about what their firms are doing to protect themselves from cyberthreats.

Daniel Garrie, co-head of the cybersecurity practice at New York's Zeichner Ellman & Krause, works with law firms and banks on privacy protection. He said it's not always the top-tier firms that have the best systems in place.

"The irony is, it's not a matter of how good your law firm is, it's about how strong your technology resources are," Garrie said. Earlier this year he co-authored a cybersecurity column for sibling publication Corporate Counsel riffing on an episode of CBS' "The Good Wife," where a fictional law firm is faced with a cybsecurity threat ordering it to pay $50,000 or face the deletion of all its electronic client files. ■

cyberSecure
PRODUCED BY ALM

CyberSecurity for Real Estate Pros: Why, Where to Start

By Rayna Katz, GlobeSt.com

The time has come to pay attention to cyber security—the focus of the upcoming cyberSecure conference here in December. Yet the real estate industry has been surprisingly slow to sit up and take notice.

"This is a real threat, it's not hypothetical and the impact is staggering," declares Jodie Kelley, SVP and general counsel, BSA | The Software Alliance. "Symantec [a cyber security tool provider] estimated a million new threats were created each day in 2014. On average, an organization experiences a cyber threat every seven minutes. Someone may not get in to a company's system but the issue is pervasive and a lot isn't even visible to companies."

But commercial real estate firms have been slow to jump on the bandwagon. "They're interested in making deals and collecting rent," says Jim Ambrosini, managing director at industry accounting and consulting firm CohnReznick Advisory and a cyber security specialist. "In general, information technology takes a back seat."

"Only now," he continues, "are CRE firms looking at this because of all the news and they may have board members or an investor asking 'Are you secure?' So they're doing assessments and we're finding dozens, if not hundreds, of vulnerabilities."

And there's a lot riding on those assessments, Ambrosini asserts. "There's pending deal information, potential trade information and more. In one instance of a cyber security breach that we saw, an email system was hacked and it was used to analyze patterns of communication. From there, the hackers sent a letter, seemingly from the CEO, to the CFO requesting a wire transfer of several million dollars. It went through and was stopped only by the bank."

> *'There's no tolerance today for a lack of fiduciary duty around cybersecurity.'*
>
> —Jim Ambrosini
> CohnReznick Advisory

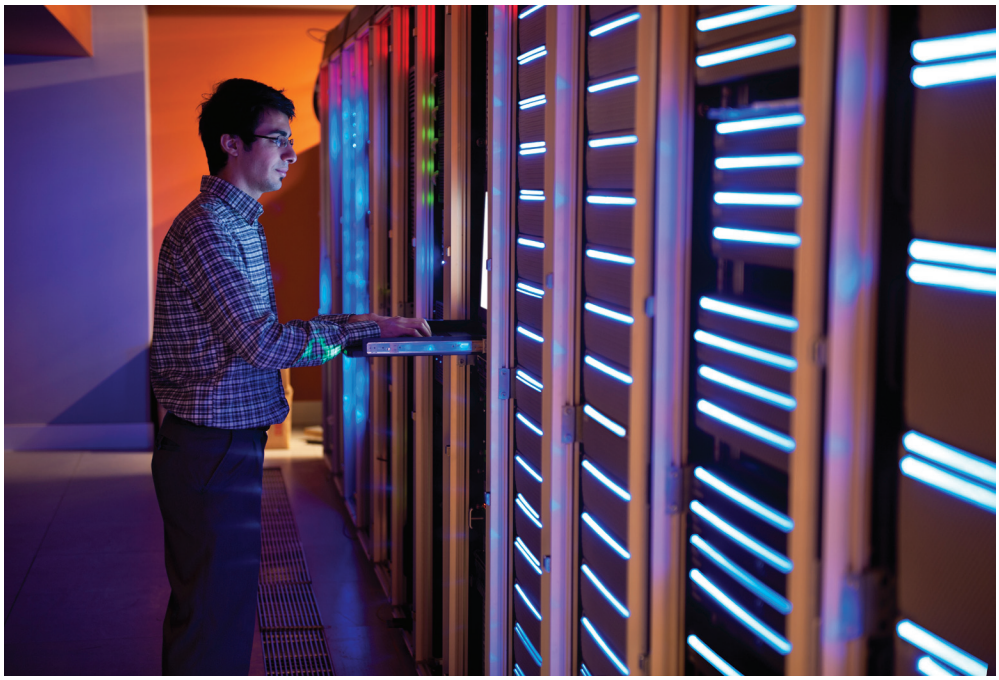
Further, he continues, "The even bigger risk is reputational. Once word of a breach gets out, a company's reputation becomes tainted. There's no tolerance today for a lack of fiduciary duty around cybersecurity. It's going to make doing business with this company a lot more difficult because the repair—including fines, legal fees, bringing in consultants and more—causes a tremendous amount of disruption."

Some C-suite executives know the problem needs to be addressed but they're not sure where to begin. The first step, experts say, is to take stock of your situation. "The very first thing we recommend companies do is look at their own network and see what's running on it," advises Kelley. "People see threats as external but a lot of companies we've worked with don't know what they have in their network. They don't have a good inventory of their software and/or licenses, so they can't get all of the security patches they need."

Next, advises Mark Stamford, founder and CEO of OccamSec, "Look at what other industries—such as retail—have done. That's the most important thing for real estate firms, instead of starting from scratch."

However, he cautions, "You have to consider the specifics of your industry and how it may be targeted. You can't just blindly copy what someone else is doing." Then, put tools in place, but choose very carefully.

"Information security is driven by FUD-fear, uncertainty and doubt," warns Stamford. "But people have to reel that back and keep a check on what's going on because there is a lot of hype. It pays to do some due diligence before throwing money at this problem." ■



As Cybersecurity Booms, So Do Investment Opportunities

Where the Real Cybersecurity Risk Comes From

ThinkAdvisor

A report by Bank of America Merrill Lynch examined investment opportunities for firms in the cybersecurity space.

The market itself is large and growing. Citing data from technology research firm Gartner, BofA estimated the cybersecurity solutions market is currently between $75 billion and $77 billion. It's expected to grow to $170 million by 2020, according to market research firm Markets and Markets.

A big reason for that growth is corporate spending on cybersecurity, especially in the financial services industry, as well as telecoms, technology and manufacturing. "Cyberspend," as BofA put it, budgets have grown nearly twice as fast as IT budgets over the past two years, and firms are spending an average 6% of their overall IT budget on cybersecurity initiatives, compared with 2% in 2010.

The Securities Industry and Financial Markets Association, for its part, recently carried out a cybersecurity exercise called Quantum Dawn 3, with more than 80 participants in the financial sector and government.

Investors are finding increasing opportunity to invest in the cybersecurity market. Cybersecurity startups raised $2.5 billion in 2014 across 224 investments, according to BofA, and there have been 59 M&A transactions between cybersecurity firms. Cybersecurity-related unit investment trusts and ETFs, like PureFunds' Cyber Security ETF (HACK) are also entering the market.

Low-growth areas in the cybersecurity market include endpoint protection platforms and consumer security software, which combined account for 39% of the market, but those are offset by better performance in the security information and event management (SEIM), secure Web gateway, identity governance and administration and enterprise content-aware data loss prevention areas.

Software is the largest segment in the cybersecurity industry, BofA found, at $21.4 billion. It's expected to reach nearly $27 billion by the end of the decade, driven primarily by new freemium models, security appliances, and increased security for cloud operators and mobile devices.

The enterprise market, which serves firms rather than consumers or end users, represents about $15 billion and is forecast to grow to $19.5 billion by 2018. The endpoint security market is expected to grow from $10 billion in 2014 to over $14.5 billion five years later.

By revenue and market share, Symantec is the largest security software vendor, with $3.7 billion in 2014 and 17% market share. However, even though IBM is only the third largest vendor by those measures, growth from 2013 to 2014 far outpaced its competitors: 17% compared with 4.6% for Intel and 5% for EMC.

Much of IBM's growth is driven by SEIM solutions, according to the report. "Security information and event management (SIEM) is defined as applying security analytics to real time events for the detection of targeted attacks and data breaches, and hence logging these for reference to prevent future attacks in an enterprise environment. It is considered a mixture of both software and serviced-based cybersecurity solution."

According to the research firm MarketsandMarkets, the SEIM sector is expected to grow from less than $3 billion in 2014 to $4.5 billion in 2019 at a compound annual growth rate of 12%, the highest for any of the sectors in the cybersecurity market.

It's the little guys that are leading in innovation, though. Business development firm Cybersecurity Ventures rated firms like FireEye, an advanced threat protection provider, and Lancope, which provides network visibility and security intelligence, as the most innovative in the industry. Only IBM and Lockheed Martin were in the top 10.

The report found adopting new technologies is the biggest priority for corporations' cybersecurity budgets, followed by audits and assessments of current systems. However, only a third of executives surveyed by PwC said they prioritized adding new skills and capabilities along with that new technology.

Governments are also increasing what they spend on cybersecurity. In the United States, the number of information security incidents increased from over 5,500 in 2006 to 67,168 in 2014, according to data the report. "In response, the U.S. federal government spent $78.8 billion in total on cybersecurity between 2006–2013, and this is expected to reach $14 billion in 2016 alone."

In spite of that, BofA believes the government is still not spending enough. "Despite seemingly facing an increasing wave of attacks, spend on cybersecurity as a percentage of total department budget is still low," it wrote in the report. "In fact, only the Department of Homeland Security spends more that 3% of its 2014 budget on cybersecurity."

The report noted that there are seven factors that influence the cost of a data breach to a company: third-party errors, lost or stolen devices, quick notification, a strong security posture, incident response planning, appointing a chief information security officer and consulting support.

In fact, companies that deployed a security intelligence system had an estimated 21% retun on investment. Estimated ROI for encryption technology was 18%, followed by firewalls at 14%. ■

cyberSecure PRODUCED BY ALM

December 15-16, 2015 The Sheraton Times Square, New York, NY

ALM cyberSecure is a two-day event designed to unite business leaders and the entire risk management team. Sessions and workshops will provide attendees with the insights and connections necessary to implement a preparedness and response strategy that changes the conversation from financial risk to competitive advantage.

Agenda highlights include:

- **Six Keynote Presentations on Topics including:** Pro-Activity, Protection, Sound the Alarm, Prevention, Public Policy, and What Actually Works?
- **Tracks Include:** Legal, Technology, Insurance & Risk, Government, Deep Dive Workshops
- **'How Hacks Happen'** Showcase Competition
- **Morning Briefing:** Industry Trends in Cybersecurity Practices with ALM's Market Intelligence Analysts
- **Earn Credits:** CLE, CPD/CPE, CE Credit Eligible Content!

Here is your opportunity to be a spectator as cybersecurity defenders battle to protect their networks as rival cyber attackers try to break through. Organized in collaboration with Vermont Law School and The Center for Infrastructure Assurance and Security, University of Texas San Antonio, don't miss this live action cybersecurity competition where teams of college students will compete against each other for control of a resource that must be protected against ongoing attacks from members of rival teams.

Cyber Clinics

Choose from Four 45-minute Cyber Clinics providing targeted solutions to universal dilemmas including:

- Who to call and what to ask when a breach occurs
- The root causes of major breaches and how to avoid them
- How the activities of international cybercriminals are poised to impact your business
- Choosing how to emphasize technological versus insurance based solutions to cyberrisks

Be among the first to hear Industry Trends in Cybersecurity Practices – the results of proprietary research presented by ALM Legal Intelligence analysts will be revealed only at cyberSecure

Who Should Attend

Executive Management, Legal Counsel, IT & Technology, Risk Managers, Insurance Carriers, Broker & Agents, Finance Executives, Consultants

For more information visit www.almcybersecure.com and phone Frank Wolson at 212-457-9510 to receive a special discount.

Confirmed Speaker Faculty List:

Andrea Arias, Attorney
Federal Trade Commission, Division of Privacy and Identity Protection

Austin Berglas, Senior Managing Director – Head of US Cyber Investigations and Incident Response
K2 Intelligence

JoAnn Carlton, General Counsel and Corporate Secretary
Bank of America Merchant Services

John Farley, Vice President, Cyber Risk Practice Leader
HUB International

Tom Finan, Senior Cybersecurity Strategist and Counsel
US Department of Homeland Security

Jason Gonzalez, Partner, Practice Group Leader, Data Privacy & Cybersecurity
Nixon Peabody

Tom Kellermann, Chief Cybersecurity Office
Trend Micro

David Lashway, Partner
Baker & McKenzie LLP

Richard Levick, Chairman & CEO
LEVICK

Michelle Lopilato, Director of Cyber and Technology Solutions
HUB International

Edward J. McAndrew, Assistant United States Attorney
Cybercrime Coordinator, U.S. Attorney's Office, District of Delaware

Jason Maloni, Senior Vice President; Chair, Litigation Practice
LEVICK

Richard Martinez, Partner; Chair, Privacy and Cybersecurity Litigation;
Robins Kaplan

John Mullen, Managing Partner of the Philadelphia Regional Office and Chair of the US Data Privacy and Network Security Group
Lewis Brisbois Bisgaard & Smith

Mauricio Paez, Partner
Jones Day

Vince Polley, Principal
KnowConnect PLLC

Mark Sangster, Vice President, Marketing
eSentire Inc.

Shahryar Shaghaghi, Managing Director
BDO Consulting

Bill Sieglein, Founder
CISO Executive Network

Rick Shutts, CISSP, CRISC, Chief Information Officer
Harris Beach PLC

Lisa Sotto, Partner
Hunton & Williams

Brookes Taney, Vice President of Data Breach Solutions
Epiq Systems

Mercedes Tunstall, Partner
Pillsbury Winthrop Shaw Pittman LLP

Danielle Vanderzanden, Shareholder; Co-Chair of the Firm's Data Privacy Practice Group
Ogletree Deakins

Alan Winchester, Member
Harris Beach PLLC