SOCIAL MEDIA

U.S. and European Lawmakers Scrutinize Facebook

Facebook continues to draw fire from its users, privacy groups, and some lawmakers in both the United States and Europe. The uproar this time is over the recent disclosure of a blind research study the social network site conducted one week in January 2012, unbeknownst to its subscribers. Essentially, Facebook manipulated the content of news feeds being sent to 700,000 users to see if negative emotions were contagious. The researchers' published the study's findings in the *Proceedings of the National Academy of Science (PNAS)* and stated that "the actual impact on people in the experiment was the minimal amount to statistically detect it." The reaction to the survey after the fact was anything but minimal.

Several European data protection agencieshave expressed their concern that the survey constituted a breach of users' privacy. Similarly, at least one U.S. privacy group registered a complaint with the Federal Trade Commission (FTC), and Senator Mark Warner (D-Va.) asked the FTC to "explore the potential ramifications" of the study.

"As the collection and analysis of 'big data' continues to increase, and as it assumes a larger role in the business plans of Internet-based companies, it is appropriate that we consider questions about what, if any, oversight might be appropriate, and whether best practices should be developed and implemented by the industry or by the FTC," wrote Warner.

Warner acknowledged that "companies like Facebook may have to perform research on a broad scale in order to improve their products. However, because of the constantly evolving nature of social media, big data, and the Internet, many of these issues currently fall into unchartered territory."

INFO SECURITY

Congress Asked to Help Protect Consumers' Data

The Federal Trade Commission (FTC) recently asked Congress to do more to protect consumers against the unchecked collection and sharing of their digital data by providing them with tools to view, suppress, and change their information. The agency also asked Congress to rein in data brokers, the companies that analyze and sell huge amounts of information for marketing purposes.

The FTC took aim at the data brokerage industry in its recent report to Congress, "Data Brokers: A Call for Transparency and Accountability." There is a fundamental lack of transparency about data brokers' practices, the agency noted in the exhaustive report. Unbeknownst to most consumers, data brokers work behind the scenes to gather information about them from commercial, government, and other publicly available sources both online and offline. From this, they can create a composite of the consumer that can infer race, gender, or sexual orientation, among other things – a composite that could, in actuality, be flawed. Storing this type of data indefinitely, the FTC pointed out, also poses a security risk.

An earlier report released by the White House raised similar flags regarding the immense aggregation of personal information. According to an article in *The New York Times*, the report's most significant findings focused on "the recognition that data can be used in subtle ways to create forms of discrimination and to make judgments – sometimes in error – about who is likely to show up at work, pay their mortgage on time, or require expensive medical treatment."

PRIVACY

Florida Passes Far-Reaching Data Security Law

The state of Florida has enacted a new law that increases security accountability for all business, healthcare, and governmental entities that reside or do business in the state. The new Florida Information Protection Act of 2014 (FIPA) specifically requires organizations to take reasonable measures to protect personal information, the definition of which has been broadened to include an individual's first name, first initial and last name, or any middle name and last name, in combination with a Social Security, driver's license, account, credit card, or debit card number.

Healthcare organizations take note: the law also expands the definition to include health insurance policy or subscriber number or any unique identifier used by a health insurer to identify the individual; information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis; or financial information. Further, it encompasses third-party agents that collect, maintain, store, or use personal information of Florida residents.

Healthcare organizations that operate in Florida will need to abide by both the Health Insurance Portability and Accountability Act (HIPAA) and the state's stringent data privacy laws, Jennifer Christianson, a partner at the law firm Carlton Fields Jorden Burt, told *InformationWeek*. One notable variance is in the number of days organizations have to notify affected individuals and the Florida attorney general. If a third-party service provider experiences the breach, the healthcare organization – not the third-party organization – is responsible for notification.

Christianson stressed that healthcare organizations must ensure that their business associates and other partners comply with privacy rules, and that all organizations must review their insurance policies to ensure breaches are covered. Failure to comply would be risky and potentially very expensive.

CYBERSECURITY

Apple to Team with IBM

And they said it would never happen. Apple recently announced that it was teaming with its former nemesis to bring IBM's big data and analytics capabilities to iPhone® and iPad®. Together they will develop more than 100 industry-specific applications, developed from the ground up, for the two devices.

Apple said the partnership will redefine the way work will get done, address key industry mobility challenges, and spark true mobile-led business change. Specifically, the two companies intend to deliver the essential elements of enterprise mobile solutions:

- Mobile solutions that transform business – The companies will collaborate to build IBM MobileFirst for iOS Solutions – a new class of "made-for-business apps" targeting specific industry issues or opportunities in retail, health care, banking, travel and transportation, telecommunications, and insurance, among others. The apps will become available starting this fall.
- Mobile platform – The IBM MobileFirst Platform for iOS will deliver the services required for an end-to-end enterprise capability, from analytics, workflow, and cloud storage, to fleet-scale device management, security and integration.
- Mobile service and support – AppleCare for Enterprise will provide 24/7 customer support to IT departments and end users while IBM will deliver onsite service.
- Packaged service offerings – IBM is introducing IBM MobileFirst Supply and Management for device supply, activation, and management services for iPhone and iPad, with leasing options.

CLOUD

EU Issues Cloud Guidelines

The European Commission (EC) has released guidelines intended to increase professional users' trust in cloud technology and to standardize service level agreements (SLAs). The guidelines were developed by the Cloud Select Industry Group (C-SIG) as part of the Commission's European Cloud Strategy. Contributors included ATOS, Cloud Security Alliance, ENISA, IBM, Microsoft, SAP, and Telecom Italia.

According to the EC, the guidelines are the first step toward standardizing SLA terminology and metrics. They will help business cloud users ensure that the key elements regarding technical and legal aspects of the services provided are included in plain language in their contracts with cloud providers. Examples of the essential items that need to be included are:

- The availability and reliability of the cloud service
- The quality of support services the user will receive from the cloud provider
- Security levels
- How to better manage the data stored in the cloud

The next step is to test the guidelines with users, particularly small and mid-size businesses. C-SIG is also working with the ISO Cloud Computing Working Group "to present a European position of SLA standardizations."

PRIVACY

Europe Turns Up the Heat on Google's Privacy Policy

It's taken more than two years and two appeals, but a privacy class action suit filed against Google in 2012 will be moving ahead, at least in part. The suit was filed in response to Google's adoption of a single, unified policy that allowed it to commingle Android users' data across all accounts and to provide that data to third-party advertisers.

After evaluating each claim of each sub-class in the suit, a California court allowed two claims, which include U.S. users who acquired an Android device and downloaded at least one application through the Android Market or Google Play between August 19, 2004, and the present, to proceed. Claims filed by users who acquired an Android device between May 1, 2010, and February 29, 2012, but switched to a non-Android device on or after March 1, 2012, were dismissed.

According to *IDG News*, the claims allowed include one that alleges Google breached its contract with the users by disclosing data to third parties following every download or app purchase. A second claim is filed under California's Unfair Competition Law.

European Union member countries also have taken Google to task over the 2012 policy change. Although Google has made changes to the offending policy, European data protection regulators are not satisfied. Italy is the latest country to join the fray. In late July, Italy's data protection commissioner, who has reportedly been coordinating with his counterparts across the EU, announced that Google had 18 months to comply with the European data protection law. Specifically, Google must make the following changes or, according to IT news service Gigaom, face possible criminal charges and fines of €1 million ($1.35 million U.S.):

- Make it clear to users that their data is mixed and matched across Google services for marketing purposes, both by cookies and by more advanced behavioral "fingerprinting" technologies.
- Get explicit opt-in permission from users before using their data in this way.
- Define how long it retains users' data.
- Delete users' data when asked, within two months for data stored on "active" systems and within six months for backed-up data.

By the end of September, Google must submit a plan outlining the steps it will take to comply.

CYBERSECURITY

Cyber Crime Costs More Than $400B Annually

A new McAfee-sponsored report from the Center for Strategic and International Studies (CSIS) revealed that cyber crime is having a significant impact on economies around the world. More specifically, it has cost businesses worldwide between $375 billion and $575 billion, more than the national income of most countries. Governments and companies underestimate how much risk cyber crime poses and how quickly that risk can grow, asserted CSIS.

The full impact of cyber crime, of course, goes beyond the dollar figure. It is also being felt in the job market. CSIS estimated that the losses from cyber crime could cost as many as 200,000 jobs in the United States and 150,000 jobs in the European Union.

The most important cost, however, is the damage to company performance and national economies, the report asserted. It damages trade, competitiveness, innovation, and global economic growth. Specifically:

- The cost of cyber crime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.
- Cyber crime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.
- Governments need to begin serious, systematic effort to collect and publish data on cyber crime to help countries and companies make better choices about risk and policy.

It's imperative, therefore, that companies do more to protect their networks and countries strengthen their cyber defenses. What is needed, CSIS contended, is better technology and stronger defenses, as well as agreement and application of standards and best practices.

"Making progress on these changes will require governments to do a better job accounting for loss and companies to do a better job assessing risk," the report concluded.

BYOD

BYOD May Relieve Some E-discovery Headaches

Employers are realizing that they aren't always able to prevent their employees from using their personal devices for work purposes while on the job. A global survey by Fortinet found that 70% of personal account holders have used their personal cloud storage accounts for work purposes. This can present a problem when a lawsuit involves e-discovery of company documents, more and more of which are being created on personal devices or stored in personal Internet spaces.

One solution that some companies are exploring is mandatory BYOD. Yes, in the very near future you may be required to provide your own smartphone, tablet, or computer. Gartner has predicted that 50% of employers will require employees to supply their own devices for work purposes by 2017.

Gigaom's Geoffrey Goetz pointed out in a recent article that such a move would necessitate adjusting the company's privacy policy. Employees would also have to surrender their personal devices when it is legally in the company's best interest to do so if the goal of the mandatory BYOD policy includes helping to manage the risk associated with complying with e-discovery requests when the data resides on an employee's personal device.

Clearly, mandatory BYOD needs to be a carefully thought-out step for any organization.

CLOUD

Study: Mobile Users Shape the Cloud Computing Landscape

Thanks in lareg part to the increasing use of mibile devices for business purposes,the majority of the companies in the United States and Europe have made the move to the cloud, according to a new study by Frost & Sullivan. Although U.S. organizations lead Europeans in the rate of cloud adoption, companies in both regions are clearly becoming more aware of the benefits of the cloud.

More than half the businesses surveyed have already moved 50% or more of their enterprise communications solutions – particularly e-mail servers and collaborative applications – to the cloud. A quarter of those companies expect that percentage to increase to more than 75% over the next three years.

The study determined that 57% of U.S. and European cloud users are "cloud reliant." Furthermore, 70% of U.S. and 56% of European respondents currently using cloud technologies find them to be highly effective, indicating that increased exposure to cloud technologies could lead to wider adoption. The majority of cloud-reliant users are in the United States, particularly in manufacturing and in businesses of 20-500 employees and businesses of more than 10,000, according to Frost & Sullivan Research Analyst Karolina Olszewska. In the future, the largest growth areas will likely be the government sector and small businesses.

"The share of remote and mobile workers is expected to increase over the next three years and change business technology requirements," concluded Olszewska. "The cost impact of supporting these new business needs will be felt more intensely by IT decision-makers in the United States than those in Europe."

PRIVACY

Data Privacy Becomes an HR Issue

Until lately, data privacy has been regarded as primarily an IT issue. Some – particularly in the legal community – contend it is also becoming a human resources issue as hackers are starting to take aim at employee personal information as well as customer information. Take the monstrous Target breach as an example. The hackers attacked both customer and employee personal data.

In the Connecticut Employment Law Blog, publisher Daniel Schwartz, a partner at Shipman and Goodwin LLP, also noted an article in *The New York Times* that reported hackers recently tried to access government employee files that included in-depth personal information required for security clearances. Four months later, the administration says there is no indication that the breach was successful.

The motivations for the attacks may be different, but both instances drive home Schwartz's point that HR departments have some skin in the game of data privacy. He recommended that HR develop a data privacy policy to cover security concerns; continually train and educate all employees – including senior executives – on the steps they need to take to protect confidential information; conduct regular audits of information in all formats, including paper; and insert clauses into employment contracts that clearly prohibit employees from accessing confidential data during their employment with the company and after they leave.

PRIVACY

Europe and Canada Embrace Right to Be Forgotten

The right to be forgotten (RTBF) is gaining ground. Both Europe and Canada have implemented RTBF regulations and are looking at extending it beyond national boundaries.

Europe's RTBF regulations went into effect May 30, and by July 3 Google already had received nearly 70,000 requests to remove links to content on some of the world's largest news sites. The European Court of Justice, the highest court in the European Union, ruled in June that European users should have the right to be forgotten on the Internet. It decided there were certain cases in which Google and other Internet companies should allow online users to be "forgotten" after a certain time by erasing links to web pages "unless there are particular reasons, such as the role played by the data subject in public life, justifying a preponderant interest of the public."

Thus, Google and other Internet companies would have to remove web pages if requested, even if the original "publication in itself on those pages is lawful." If the provider doesn't remove the link to the "offending" information, the user can take the matter to the appropriate authorities to obtain, under certain conditions, the removal at the Internet company's expense. The officials will then weigh "legitimate interest of Internet users potentially interested in having access to that information" and the individual's fundamental right to privacy and to the protection of personal data. The decision to remove links, according to the court, would depend on the "nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."

BBC News Business Economics Editor Richard Preston announced to readers on July 2 that BBC had received notice from the search giant that it would no longer be able to show a blog Preston wrote in 2007 in response to certain searches on European versions of Google. There was no additional information provided, including why the link was no longer going to be available via the search engine. Had the individual who was the main subject of the news item requested its removal? After some sleuthing, Preston discovered that the removal was prompted by a request from a reader who chose to comment on the article. For whatever reason, he no longer wanted his comment to be visible under the provisions of the new RTBF regulation.

BBC News isn't the only news site already affected by the new regulations. World news agency AFP (Agence France-Presse) reported that the UK's *The Guardian* also had received notices that six of its articles would no longer be included in European search results. A few days later some of the links were restored, a clear indicator that Google is refining its processes as it goes.

In the meantime, European users conducting Internet searches using Google and other search engines may not receive a complete list of references. That doesn't mean the content no longer exists or is unavailable, however. It still exists on the news sites – complete with comments. Apparently, the restrictions also relate only to certain search terms. The removed links also continue to show up in search results on the U.S. version of Google.

European news agencies are predictably extremely unhappy with Google's actions, which the search company contends are necessary for compliance with the court's order. *Mail Online* publisher Martin Clarke says the instances to date show what a nonsense the right to be forgotten is. "It is the equivalent of going into libraries and burning books you don't like," he contended. He told AFP that *Mail Online* would regularly publish lists of articles removed from Google's European search results. The BBC and *The Guardian* also published links to the restricted stories.

A Google spokesperson told AFP that it individually examines each request to be forgotten to determine whether it meets the court ruling's criteria. "This is a new and evolving process for us," she said. "We'll continue to listen to feedback and will also work with data protection authorities and others as we comply with the ruling."

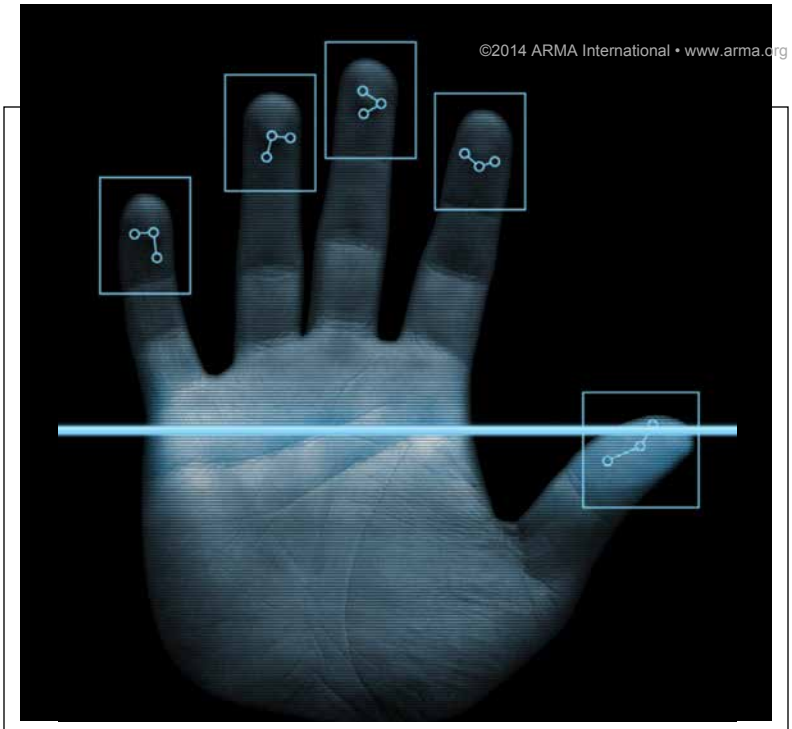
INFO SECURITY

The Sedona Conference® Adds Data Security Working Group

The Sedona Conference® has established Working Group 11 (WG11) to focus on data security and privacy liability. The group's mission is to identify and comment on trends in data security and privacy law so that organizations may better prepare for and respond to data breaches. It will also provide guidance regarding data security and privacy class-action developments, including liability, damages, and class certification issues.

WG11 will be guided by a steering committee composed of representatives of the various stakeholders involved in the data security and privacy liability area. Anyone interested in this subject is welcome to join the full group, which will meet virtually, with limited face-to-face meetings throughout the year, the first of which is scheduled for November 5-7 in New Orleans.

The Sedona Conference® describes itself as a nonprofit research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. It is known for bringing together some of the brightest minds to create practical solutions and recommendations of immediate benefit to the civil justice system. It has 11 working groups that use an extended peer-review process to develop content that is widely published in conjunction with legal and professional educational programs.



CLOUD

NIST Drafts Cloud Forensic Standard

The increased use of cloud computing brings new and bigger challenges for those involved in digital forensics. As the National Institute of Standards and Technology (NIST) recently pointed out, "The characteristics that make this new technology so attractive also create challenges for forensic investigators who must track down evidence in the ever-changing, elastic, on-demand, self-provisioning cloud computing environments. Even if they seize a tablet or laptop computer at a crime scene, digital crime fighters could come up empty handed if these devices are linked to pooled resources in the cloud."

NIST's Cloud Computing Forensic Science Working Group, an international body of cloud and digital forensic experts from industry, government, and academia, set out to identify the challenges that cloud computing poses to forensics investigators who uncover, gather, examine, and interpret digital evidence to help solve crimes. The group's recent report, "NIST Cloud Computing Forensic Science Challenges," identified 65 such challenges. While the report focuses on the technical challenges, almost all intersect with legal and organizational issues. The group divided the 65 challenges among nine categories, including architecture, data collection, analysis, standards, training, and "anti-forensics" (such as data hiding and malware).

"The long-term goal of this effort is to build a deeper understanding of, and consensus on, the high-priority challenges so that the public and private sectors can collaborate on effective responses," said Martin Herman, co-chairman of NIST's Cloud Computing Forensic Working Group.

NIST believes there is a pressing need to develop forensic protocols that major cloud providers eventually would adopt. "These protocols must adequately address the needs of the first responders and court systems while assuring the cloud providers no disruption or minimal disruption to their services," the report stated.

INFO SECURITY

Too Small for a Cyber Attack?

Small businesses don't need to worry about cyber attacks, right? After all, you only hear about large enterprises and some mid-size businesses being hacked.

While the latter statement is true enough, that doesn't mean small businesses aren't at risk, particulary given their reliance on mobile devices for storing critical business information. According to the UK Federation of Small Business, 41% of small firms were victims of cybercrime – including online fraud and computer viruses – in 2013. One in 10 of micro firms (10 or fewer employees) surveyed by Kaspersky Labs admitted that an IT security breach would probably cost them their business.

"While it is encouraging to see the extent to which micro firms are embracing the latest technologies, this must go hand in hand with a strong approach to internet security," said Kirill Slavin, UK managing director at Kaspersky Lab. "Micro firms don't have to become IT security experts. Most of the time it's the IT equivalent of remembering to lock all the doors and windows when you go out, make sure you have some additional protection and not to leave valuables where others can easily see and get to them."

A survey by Barclays Bank revealed one in eight small businesses are victims of cyber-fraud each year. "Typical scams include opportunities to acquire new customers who you supply but never receive payment from, or to purchase items from new suppliers that never deliver after having been paid. Fraud can happen to any type of business in many different ways, impacting their revenue, reputation and the long-term health of the business, with no business being too small to be targeted," said Alex Grant, Barclays managing director of fraud prevention.

Kaspersky Labs and Barclays Bank suggested that small and micro firms spend just five minutes a day checking the following five things to help keep their businesses safe:

1. Passwords – All Internet-enabled devices that carry your business data should be protected by strong passwords, whether the equipment is company- or employee-owned.
2. Attachment awareness – Understand the dangers that can lurk in e-mails, web links, USB sticks, CDs, etc., and onsider introducing extra software that will filter out or contain suspicious-looking items.
3. Educate all employees – Make sure everyone knows how to stay safe online, including how to use strong passwords, spot suspect e-mails or sites, and protect company information.
4. Back-up – Every day make sure the information you store on computers is backed-up and secure.
5. Security systems – Take full advantage of any user-friendly Internet security software that has been specially created for small firms to secure devices such as smartphones, laptops, tablets, computers, WiFi, and networks. Also remember to keep things out of sight and the site locked up.

PRIVACY

Consumers: Access to EHR Trumps Privacy

The ability to access electronic health records (EHR) outweighs concerns of privacy invasion for U.S. consumers with chronic conditions, according to a report from Accenture. The research study of 2,011 individuals, a little more than half of whom had a chronic condition, revealed that 69% of those with a chronic condition believe they should have the right to access all of their healthcare information, and 51% believe that accessing their medical records online outweighs the privacy risks.

The biggest barrier to accessing those records online for 55% of those with chronic conditions is not knowing how to do it. For the largest majority (87%), access isn't enough; they want to control their health data. Only a little more than half, however, believe they have much or any control over their medical information.

The U.S. Centers for Disease Control estimates that 47% of Americans have at least one chronic disease, but they account for 76% of all physician visits. They are also actively engaged at most stages of patient care, which means health care needs to adapt to a new generation of consumers who expect to have transparency and therefore demand more access to their personal data online, said Kaveh Safavi, M.D., J.D., the leader of Accenture's global health business.

Privacy Concerns Among U.S. Consumers with Chronic Conditions

Individuals are slightly less concerned about the privacy of their electronic medical data (65%) than other personal information that is stored electronically, such as online banking (70%), in-store credit card use (69%), and online shopping (68%), according to an Accenture survery.

Source: Accenture Patient Engagement Survey, 2014

COPYRIGHT

Europeans Call for a Single Copyright

The European Commission (EC) received an earful when it asked for public comment on the EU copyright rules earlier this year. It seems many European consumers want a single EU copyright. They are frustrated with being denied cross-border access to online content, especially when attempting to view or listen to content from their home country when they are in another EU country. In other words, they want a single market in which they can access all content from any online stores whether directed to the member state in which they reside or not. Those that called for a common copyright believe that it would do away with territorial restrictions and allow users to freely access, purchase, and transfer content across the entire EU market.

Libraries expressed sentiments similar to those of consumers. University libraries especially pointed to problems students face in trying to access online educational resources from sources – including other universities – outside the country in which they are searching.

Those generating and publishing the content, however, laid the blame on the service providers. EU-wide cross-border licenses are available; it's the digital providers who limit the access, they contended. Film producers and broadcasters see territoriality as less of an issue, in large part because of language differences.

The EC reviewed more than 2,000 responses in composing a white paper that examines whether further action on the current EU copyright system is needed. That paper is expected this fall.

INFO GOVERNANCE

New Risk Maturity Index Emerges from Study

A recent PricewaterhouseCoopers (PwC) study found that most organizations (almost 60%) in Europe and North America are aware of the importance of their information and its role in gaining competitive advantage. The challenge is protecting it from internal and external threats without sacrificing its access and value within the organization.

"The repeated emphasis from regulators, advisors, and risk-managers on data protection and information safeguarding has become the holy grail of data management," observed PwC analysts in the report. "Unfortunately, this company-wide focus on security has kept organizations and their boards from sharing and distributing data and information within the organization to maximize its value."

The study, commissioned by Iron Mountain, is in its third year, but this is the first year it presented the results in a risk maturity index. The index gauges the extent to which businesses implement and monitor a set of 34 measures to manage and protect information assets. These measures fall into four groupings: strategy, people, communications, and security. To receive a high individual index score, an organization must not only implement the measure but also monitor its effectiveness. The four levels of risk maturity are:

- Unprepared for Risk – Organization is severely exposed to information risk. It likely does not have an information risk strategy in place, and senior management is unaware of the potential impact to its business. (Score: 49 or under)
- Aware of Risk – Organization realizes it needs to manage risk but is uncertain about what to do or remains ill-equipped to tackle the threat. (Score: 50-79)
- Approaching Maturity – Organization has established some measure and senior leaders are more aware. It has reduced its exposure but has not yet implemented a robust strategy. (Score: 80-99)

- Equipped for Risk – Organization has implemented a responsible approach that encompasses strategy, people, communications, and security from top to bottom. It monitors, evaluates, and improves its approach to effectively manage its exposure to risk. (Score: 100)

Larger organizations (2,500+ employees) are outperforming mid-size organizations (250-2,500 employees) in this effort, with Europe leading the United States. Businesses in Norway stand out from the other countries (United States, Canada, France, United Kingdom, Germany, Spain, the Netherlands, and Hungary), followed by France and Canada. According to the report, businesses in these countries stand apart from the others because they understand the importance of monitoring the effectiveness of their strategies and making the necessary changes to keep ahead of the risk. At the sector level, energy and pharmaceutical businesses lead the way in information risk strategy in both Europe and North America.

Those organizations that are leading the pack and approaching maturity are focused on monitoring the success of their policies and programs and adapting to the evolving landscape. They are more likely to have prioritized leadership, communications, and analytic skills in future growth plans. Further, they protect their data well but also use that data to drive growth through innovation.

"The key to the success of information risk initiatives is to build both the policy and the evaluation into the day-to-day processes," PwC concluded. For some organizations, this may require a significant cultural shift.

CYBERSECURITY

Needed: Cybersecurity Professionals

The need for skilled cybersecurity specialists has grown exponentially as governments and businesses have raced to protect their networks from cyber attacks from all directions. Unfortunately, the supply doesn't begin to meet the demand, which some believe could become a national security issue.

"We do see a lack of capability and capacity in skilled professionals, and that's partly due to massive demand across the world that stretches an already small, existing pool of people," Bryce Boland, Asia Pacific chief technology officer at California-based FireEye Inc., a cybersecurity firm, said in a recent *Bloomberg Businessweek* interview.

Unfortunately, addressing this gap between supply and demand takes time. Rand Corp. explored the state of the cybersecurity labor market in its research report "Hackers Wanted: An Examination of the Cybersecurity Labor Market." It concluded that there has already been a large increase in education, particularly government-supported education, and an increase in the number of computer science majors in response to early indications of a growing demand for cybersecurity professionals.

"It's normal for the labor market to lag demand and education initiatives," Rand said in its report. "Theory suggests and experience confirms that the market may take a long time to respond to unexpected increases in demand. In the short term, many large organizations have found innovative ways of meeting the demand for cybersecurity professionals through internal recruitment and training."

The Rand report suggested the best steps may already have been taken for addressing the shortage. "The difficulty in finding qualified cybersecurity candidates is likely to solve itself, as the supply of cyberprofessionals currently in the educational pipeline increases, and the market reaches a stable, long-run equilibrium," it concluded.

A new cybersecurity report released by the Pell Center at Salve Regina University in Rhode Island took the discussion a step further by charting a path to professionalizing the field. The key element of the proposal is the creation of a professional association for the cybersecurity industry.

"There is a widening gap between the supply and demand of qualified cybersecurity professionals," said Pell Center fellow Francesca Spidalieri, one of the authors of the report. "As schools and training institutes proliferate to meet that need, basic standards are needed to assure that someone claiming special skills actually has them." She noted that there are already excellent models – such as the American Medical Association and the American Bar Association – for professionalizing the cybersecurity workforce.

"Achieving cybersecurity is far more than a technical problem: it is fundamentally a people problem," said the report's co-author, Lt. Colonel Sean Kern, USAF. "And since cybersecurity is a people problem, there must be a people solution. This requires developing an overarching organizational framework to develop, manage, and oversee the training, education, certification, and continuous professional development of a qualified cybersecurity workforce along a career continuum, and to guide leaders across society in harnessing the right people with the right knowledge, skills, and abilities to the right challenges in a rapidly-evolving environment."

Spidalieri noted that the cybersecurity industry in the United States is "highly fragmented." She and Kerns believe that a national professional association would change that and "solidify the field as a profession." They hope their study will be a catalyst for more research and efforts to unify the industry. **END**