AGENDA

A Financial Times Service

SEC Chair Urges 'Super' Cyber Disclosure
September 29, 2017

Given the heightened public focus on cyber risk and a new SEC chair who has repeatedly emphasized the importance of cyber-risk oversight, boards should expect increasing pressure on their performance on cyber security, experts say.

SEC chair Jay Clayton, who testified before the Senate banking committee on Tuesday, told senators that the onus is on public companies to move faster to disclose information on cyber breaches.

“As I look across the landscape of disclosure, and I’ve been saying this for some time, companies should be providing better disclosure about their risk profile,” Clayton said, according to a Bloomberg report on the hearing. “Companies should be providing super disclosure about intrusions that may affect shareholders’ investments.”

Indeed, boards have ramped up their oversight of cyber-risk management over the past few years. According to a recent survey by BDO, the percentage of public company directors who say their board has increased its involvement in cyber security in the past 12 months has risen every year since 2014, from 59% to 79% in 2017, and spending has followed similar patterns.

“We think this ought to be part of an intelligent discussion around what’s the appropriate level of investment in cyber security and what are the key performance indicators associated with being able to assess our return on investment for that,” says Gregory Garrett, leader of international cyber security at BDO USA.

Appropriate KPIs include the number and severity of breaches, the cost of cyber-liability insurance and the uptime or downtime of the network, he says.

“There ought to be specific key performance indicators reported to the board to help the board, because they’re obviously not cyber-security experts, to understand the value of the cyber-security investment they’re making,” Garrett says.
According to the report, the percentage of directors who say their company has increased cyber-security spending in the past 12 months has risen from 55% in 2014 to 78% in 2017.

Ransomware attacks have also been a major concern following highly publicized global events such as the "WannaCry" attack in which hackers locked up corporate data systems and demanded payment to unlock them.

More than half of directors polled by BDO (60%) said their company is addressing ransomware through measures such as focusing on patch management and increasing data back-ups to restore data faster. Boards should also hold discussions on whether and how they might pay a ransom demand, how they might report the issue, and whether they have a relationship with their local FBI office, says BDO's Garrett.

The frequency with which boards discuss cyber security has ticked up slightly over the past few years. In 2014, 30% of boards said they receive cyber-security briefings once per year. By 2017, 36% said the same. Some 16% said they received the briefings twice per year in 2014, up to 21% in 2017. One quarter of responders said they discussed cyber security quarterly or more often in 2014, compared to 34% in 2017. The biggest shift was the percentage of directors who said they never discussed cyber security, dropping from 29% in 2014 to 9% in 2017.

According to Garrett, the frequency with which boards discuss cyber risk is often related to the company’s industry. Companies in the financial services, health care and defense and government contracting businesses tend to meet most often to discuss cyber security due to the sensitivity of the data they hold, he says.

“We think this should be an ongoing dialogue in every industry, but we think there should be a [board] briefing at least on a quarterly basis,” Garrett says.

The BDO survey is based on an August poll of 140 board members at public companies with revenues ranging from $250 million to more than $1 billion.

**WALL STREET JOURNAL**

**Survey Roundup**

*October 6, 2017*

**Making Plans For Cyber:** A survey of 140 directors on public company boards by professional services firm BDO USA found 61% said they have a breach-response plan in place, up from 45% who said they had one in 2015. Sixteen percent said they don’t and 23% weren’t sure.

**COMPLIANCE WEEK**

**Auditors Offer Ideas to Help Address Cyber-Readiness**

*October 11, 2017*

Despite the proliferation and escalation of cyber-breaches, companies and government agencies are still trying to wrap their heads around the notion that break-ins are inevitable.

Corporate boards are starting to get more engaged on the cyber-threat, says Gregory Garrett, leader of international cyber-security at audit firm BDO USA. The firm’s fourth annual poll suggests a growing share of public company directors are more involved in the effort to defend against cyber-hacks than they were a year ago, and budgets committed to cyber-defense are growing. “Each year, the level of cyber-security investment is going up,” he says.

Garrett agrees companies seem to accept that they need to devote more resources and energy to cyber-defense, but they are not entirely sure where to focus. “A lot of money is being spent, but I don’t think it’s always being spent wisely,” he says. Garrett himself advocates for investing on the human side of cyber-security, namely education and training.

To assure companies cover such simpler steps in their cyber-protection strategies, auditors are starting to gear themselves up to do what auditors do best—fact check a company’s cyber-risk activities and report on unaddressed risks. The effort is voluntary, but auditors say they’re starting to see interest grow as a way to further focus and refine cyber-risk efforts.

The American Institute of Certified Public Accountants unveiled a framework earlier this year that gives companies an avenue to a voluntary attestation that would enable them to gut check their approach to cyber-risk. It enables companies to demonstrate to boards of directors, shareholders, vendors, customers, regulators, employees, and anyone else who might have an interest that the company is identifying and addressing its most serious cyber-risks.

The framework doesn’t guide a company through identifying and mitigating its cyber-risks. That’s the job of more prominent and well-established frameworks like NIST, ISO, and several others. Rather, the AICPA framework provides a means for companies to tell their stakeholders what they’re doing to manage and mitigate cyber-threat.

With the exception of some industry-specific requirements in high-risk sectors, U.S. companies are generally not bound by much regulation when it comes to protecting private information. The European Union is further ahead with the General Data Protection Regulation that takes effect next year, setting some minimum requirements on companies to protect private data and warn those affected when a breach occurs.
CYBER-SECURITY TRENDS
According to BDO, public company boards are maintaining some cyber-security trends. See below.

As companies begin to recognize heightened expectations in the United States, auditors say the AICPA reporting framework would give companies a leg up on their competitors in demonstrating a proactive approach.

It’s similar to the third-party assurance many companies provide via “SOC” reports to customers or vendors on the soundness of internal controls for Sarbanes-Oxley purposes. Companies that rely on third parties for things like payroll or other critical services need those SOC reports to roll up into their own attestations on internal controls.

In fact, auditors are even calling the new reporting framework “SOC for cyber-security,” although the SOC stands for “system and organization controls” for financial reporting purposes.

<table>
<thead>
<tr>
<th></th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased Board Involvement</td>
<td>59%</td>
<td>69%</td>
<td>74%</td>
<td>79%</td>
</tr>
<tr>
<td>Increased Cybersecurity Investments</td>
<td>53%</td>
<td>73%</td>
<td>88%</td>
<td>88%</td>
</tr>
<tr>
<td>Incident Response Plan in Place</td>
<td>NA</td>
<td>45%</td>
<td>65%</td>
<td>61%</td>
</tr>
<tr>
<td>Cyber-Breach in Past 2 Years</td>
<td>NA</td>
<td>22%</td>
<td>22%</td>
<td>18%</td>
</tr>
</tbody>
</table>

and organization controls” for cyber-purposes rather than “service organization controls” for financial reporting purposes.

The BDO survey suggests companies struggle with how to report events that have occurred, let alone the state of a company’s readiness to protect against and respond to a cyber-hack. Industry data, for example, suggests ransomware attacks are up sevenfold in the past three years, says BDO’s Garrett, but the poll of corporate directors suggests ransomware attacks have been relatively flat. “I’m concerned board members are not aware or are not accurately reporting that a company’s been breached,” he says.

The accounting and advisory organization reports that 79 percent of public company directors surveyed are more heavily involved in cybersecurity efforts this year than they were during the 12 preceding months, and 78 percent reported to have increased company investments to defend against cyberattacks. Budgets to deal with cyber threats, on average, increased by 19 percent.

However, “despite this positive progress, the survey also found that businesses continue to resist sharing information on cyberattacks with entities outside of their company,” a press release announcing the report’s publication said. Twenty-five percent of directors, the survey shows, share information on cyberattacks with external entities—a practice that the release said “needs to become more prevalent for the safety of critical infrastructure and national security.”

According to a statement from Gregory Garrett, head of international cybersecurity at BDO, “sharing information gleaned from cyberattacks is a key to defeating hackers, yet just one-quarter of directors say their company is sharing information externally. This behavior needs to change.”

CORPORATE COUNSEL
Survey: Boards Devoting More Time, Resources to Cybersecurity
September 26, 2017

Cyberattacks have been grabbing headlines lately—from the Equifax breach to a recent incursion into the U.S. Securities and Exchange Commission’s systems for storing company filings. And it appears that companies are continuing to take notice. For the fourth year in a row, the majority of board members are becoming more involved in cybersecurity compared to the year prior, according to a new survey from BDO USA.

THESTREET
Huge Lessons Companies Should Learn From Equifax’s Data Breach
September 26, 2017

Amid a growing number of corporate cyberattacks, almost every public company can learn from the trials and tribulations that the Equifax Inc. (EFX - Get Report) board of directors and management endured following a massive security breach that compromised the personal information of 143 million Americans.

With the understanding that cyberattacks are a risk that every company faces, C-suite executives and the board of directors need have a plan in place to deal with such an incident.

According to the 2017 BDO Cyber Governance Survey, about 79% of public company directors report that their board is more involved with cybersecurity than it was 12 months ago.

“The continuing year-over-year increases in board involvement and investments in cybersecurity is extremely positive, but the percentage of businesses with breach response plans in place - although much improved from two years ago - is still far below where it needs to be,” Eric Chuang, managing director of cyber incident response at BDO USA, said.
**SECURITY INTELLIGENCE**

As Cybersecurity Awareness Increases, Information Sharing Lags, Survey Shows

October 2, 2017

Interest in security is growing among business professionals. More than three-quarters (79 percent) of company directors who responded to the "2017 BDO Cyber Governance Survey" reported a rise in cybersecurity awareness during the past year. In addition, 78 percent of executives said they had matched their investment in time with a commensurate cash injection to help defend their businesses from cyberattacks during the past 12 months.

The survey, which polled 140 corporate directors of public company boards, calculated an average rise of 19 percent in security budgets. While this boost in investment is good news, many businesses remain reticent to share vital information that can help reduce the risk of attack. Instead, organizations should look to create strong cross-business partnerships, particularly between board directors and chief information security officers (CISOs).

While board members have increased their time and cash investments in cybersecurity on an annual basis, 18 percent of directors said that their business has suffered a breach during the past two years. When it comes to incident response, 61 percent of survey participants said their company had some form of incident response strategy.

While 16 percent still have no plan at all, the number of businesses that now have a strategy in place is significantly higher than just two years ago, when only 45 percent of firms had an agreed-upon approach to incident response....

The BDO survey also asked directors about the WannaCry cyberattacks. About 60 percent of board members said their business had implemented measures to help reduce the risk of ransomware. Key strategies here include an increased emphasis on patch management (58 percent), a rise in the frequency of data backups (58 percent) and the ability to restore data more quickly (46 percent).

In the report, John Riggi, managing director of cybersecurity and financial crimes at BDO, stated that too many executives are still reticent to reveal insights that could help organizations around the world reduce the risk of a security incident. In fact, only one-quarter of company directors share information about cyberattacks with other organizations. Another 24 percent said their business did not share insights with anyone else, while more than half (51 percent) were uncertain whether their organization shared information.

Of the companies that do share information, the significant majority (86 percent) communicate knowledge with government agencies, such as the FBI and the Department of Homeland Security (DHS). While almost half (47 percent) pass insights to Information Sharing and Analysis Centers (ISACs), only 8 percent communicate with rival firms....

**+HELPNETSECURITY**

Company Directors are Increasingly Involved with Cybersecurity

September 29, 2017

According to a new survey by BDO USA, 79% of public company directors report that their board is more involved with cybersecurity than it was 12 months ago and 78% say they have increased company investments during the past year to defend against cyber-attacks, with an average budget expansion of 19 percent.

This is the fourth consecutive year that board members have reported increases in time and dollars invested in cybersecurity. Despite this positive progress, the survey also found that businesses continue to resist sharing information on cyber-attacks with entities outside of their company. Just one-quarter are sharing information gleaned from cyber-attacks with external entities – a practice that needs to become more prevalent for the safety of critical infrastructure and national security.

"The survey also reveals a significant vulnerability – the continued failure of companies to share information they have gathered from cyber-attacks. Sharing information gleaned from cyber-attacks is a key to defeating hackers, yet just one-quarter of directors say their company is sharing information externally. This behavior needs to change," said Gregory Garrett, Leader of International Cybersecurity at BDO USA.

Almost one in five (18%) board members indicate that their company experienced a data breach during the past two years, a percentage very similar to the previous two years (22%).

A majority (61%) of corporate directors say their company has a cyber-breach/incident response plan in place, compared to 16% who do not have a plan and close to 23% who are not sure whether they have such a plan. Those with plans is approximately the same percentage as a year ago (63%), but a major improvement from 2015 when 45% of directors reported having them.
79% of public company board members report that their board is more involved with cybersecurity than it was 12 months ago. The vast majority of directors (91%) are briefed on cybersecurity at least once a year – this includes 28% that are briefed quarterly and better than one-fifth that are briefed twice a year (21%). The balance are briefed annually (36%) or more often than quarterly (6%).

Surprisingly, nine percent of board members say they are still not briefed at all on cybersecurity. However, during the four years of the survey, the percentage of directors reporting no cybersecurity briefings has dropped consistently....

Unfortunately, when asked whether they share information they gather from cyber-attacks, only 25% of directors – virtually unchanged from 2016 (27%) – say they share the information externally. A similar proportion (24%) say they do not share the information with anyone and 51% aren’t sure whether they do or not.

Of those sharing information on their cyber-attacks, the vast majority (86%) share with government agencies (FBI, Dept. of Homeland Security) and 47% share with ISAC (Information Sharing & Analysis Centers). Very few (8%) share with competitors.

---

**EXECUTIVE BIZ**

**BDO USA Survey: 79% of Public Company Directors Say Boards More Involved in Cybersecurity**

*September 27, 2017*

A new [BDO USA survey](#) has found that 79 percent of board members at public companies say their boards have become more involved in cybersecurity efforts than they were in the past year.

The company [said Tuesday](#) its corporate government practice polled 140 public company directors in August for the [2017 BDO Survey on Cyber Governance](#).

The survey found that 78 percent of respondents said their organizations have increased investments in cyber defense efforts in the past 12 months and that only 25 percent of directors said their companies share cyber threat data with external entities.

"Sharing information gleaned from cyber-attacks is a key to defeating hackers, yet just one-quarter of directors say their company is sharing information externally," said [Gregory Garrett](#), head of international cybersecurity at [BDO USA](#).

"This behavior needs to change," Garrett added.

Sixty-one percent of company directors said their organizations have incident response plans in place in the event of a cyber attack, while 60 percent of respondents said their companies have initiated measures to address ransomware-related threats....

---

**INFORMATION MANAGEMENT**

**Boards of Directors Taking Active Role in Data Security**

*October 11, 2017*

Boards of directors are getting more involved in cybersecurity efforts at their organizations, and many have boosted spending on such initiatives, according to a new report from accounting and advisory firm [BDO USA](#).

More than three-quarters (79 percent) of 140 public company directors surveyed in August 2017 said their board is more involved with cyber security than it was 12 months ago, and 78 percent said they have increased company investments during the past year to defend against cyber attacks. The average budget increased 19 percent.

This is the fourth consecutive year that board members have reported increases in time and dollars invested in cyber security, BDO said.

Despite this positive progress, the survey also found that businesses continue to resist sharing information on cyber attacks with entities outside of their company. Only one quarter (25 percent) are sharing information gleaned from cyber attacks with external entities.

"The annual survey has documented the continued ascension of cyber security in corporate boardrooms, as directors are being briefed more often and are responding with increased budgets to address this critical area," said [Gregory Garrett](#), leader of international cybersecurity at [BDO USA](#).

"This year’s study also indicates that boards are aware of the expanding threat of ransomware and most of their businesses are proactively addressing this risk," Garrett said. "The survey also reveals a significant vulnerability—the continued failure of companies to share information they have gathered from cyber-attacks."
CONTACT:

AMY ROJIK
617-239-7005
arojik@bdo.com

GREGORY A. GARRETT
703-770-1019
ggarrett@bdo.com

ERIC CHUANG
202-644-5435
echuang@bdo.com

STEPHANIE GIAMMARCO
212-885-7439
sgiammarco@bdo.com

JOHN RIGGI
202-644-5420
jriggi@bdo.com

MICHAEL STIGLIANESE
212-817-1782
mstigianese@bdo.com

JEFF WARD
314-889-1220
jfward@bdo.com

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm’s individual needs.

© 2017 BDO USA, LLP. All rights reserved.