Annual Reports: How They Warn of Cyber Risk

By Bruce Sussman

Read more about the author

WED | OCT 20, 2021 | 4:30 AM PDT

Cyber risk is business risk.

We hear this at SecureWorld cybersecurity conferences on a regular basis.

But how should we communicate this risk to the business, to clients, or to investors?

For an increasing number of companies, part of that conversation is happening in quarterly and annual reports. This includes the 2021 annual report from Accenture.

Let's take a look at how the company writes on this topic.

Accenture annual report: risks we face from cyberattacks

The report from the consulting giant details the most exciting news upfront. For example, company earnings hit $50.5 billion, a 14% increase in U.S. dollars year over

Most Recent

CYBERSECURITY

They Made $30 Million Because Hackers Showed Them the Future

year. Accenture featured this earnings news on page two in a big, bold font.

However, we were most interested in seeing how Accenture articulated a particular business risk: the risk from a cyberattack—especially because Accenture was hit with ransomware this year.

On page 34 of the report, Accenture dives into the risk that cyber poses to the business. The section on cyber risk is in bold:

'We face legal, reputational and financial risks from any failure to protect client and/ or Accenture data from security incidents or cyberattacks'

Legal, reputational, and financial risks? These are the very impacts we regularly hear CISOs mention on SecureWorld webcasts.

But how does Accenture explain these cyber threats to its connected way of doing business around the globe? That's where the fine print comes in.

Here is the entire section on cyber risk from Accenture's report. We tried breaking this into bite-sized chunks. The first sections are about technology and all that could go wrong with it, up to and including cyberattacks:

> "We are dependent on information technology networks and systems to securely process, transmit and store electronic information and to communicate among our locations around the world and with our people, clients, alliance partners and vendors, and unauthorized disclosure of sensitive or confidential information, including personal data and proprietary business information.
>
> In the past, we have experienced, and in the future, we may again experience, data security incidents resulting from unauthorized access to our and our service providers' systems and unauthorized acquisition of our data and our clients' data

Most Popular

CYBER LAW

Suing the CISO: SolarWinds Fires Back

More Like This

RISK MANAGEMENT

Top 5 Ways to Defend Against Ransomware Now

> including: inadvertent disclosure, misconfiguration of systems, phishing ransomware or malware attacks.
>
> For example, as previously reported, during the fourth quarter of fiscal 2021, we identified irregular activity in one of our environments, which included the extraction of proprietary information by a third party, some of which was made available to the public by the third party."

Next, the Accenture statement specifically calls out cyber risk in the cloud:

> "In addition, our clients have experienced, and may in the future experience, breaches of systems and cloud-based services enabled by or provided by us. To date these incidents have not had a material impact on our or our clients' operations; however, there is no assurance that such impacts will not be material in the future, and such incidents have in the past and may in the future have the impacts discussed below."

This is followed by AI, IoT, and Big Data and how they can be impacted by a cyber incident or attack:

> "In providing services and solutions to clients, we often manage, utilize and store sensitive or confidential client or Accenture data, including personal data and proprietary information, and we expect these activities to increase, including through the use of artificial intelligence, the Internet of Things and analytics.
>
> Unauthorized disclosure of, denial of access to, or other incidents involving sensitive or confidential client, vendor, alliance partner or Accenture data, whether through systems failure, employee negligence, fraud, misappropriation, or cybersecurity, ransomware or malware attacks, or other intentional or unintentional acts, could damage our reputation and our competitive

> positioning in the marketplace, disrupt our or our clients' business, cause us to lose clients and result in significant financial exposure and legal liability.
>
> Similarly, unauthorized access to or through, denial of access to, or other incidents involving, our software and IT supply chain or software-as-a service providers, our or our service providers' information systems or those we develop for our clients, whether by our employees or third parties, including a cyberattack by computer programmers, hackers, members of organized crime and/or state-sponsored organizations, who continuously develop and deploy viruses, ransomware, malware or other malicious software programs or social engineering attacks, has and could in the future result in negative publicity, significant remediation costs, legal liability, damage to our reputation and government sanctions and could have a material adverse effect on our results of operations—see risk factor below entitled 'Our business could be materially adversely affected if we incur legal liability.'"

Now, the Accenture statement on cyber risk moves more directly into cyberattacks and compliance risk, including regulations around privacy:

> "Cybersecurity threats are constantly expanding and evolving, becoming increasingly sophisticated and complex, increasing the difficulty of detecting and defending against them and maintaining effective security measures and protocols.
>
> We are subject to numerous laws and regulations designed to protect this information, such as the European Union's General Data Protection Regulation ('GDPR'), the United Kingdom's GDPR, the California Consumer Privacy Act (and its successor the California Privacy Rights Act that will go into effect on January 1, 2023), as well as various other U.S. federal and state laws governing the protection of privacy, health or other personally

> identifiable information and data privacy and cybersecurity laws in other regions.
>
> These laws and regulations continue to evolve, are increasing in complexity and number and increasingly conflict among the various countries in which we operate, which has resulted in greater compliance risk and cost for us.
>
> Various privacy laws impose compliance obligations regarding the handling of personal data, including the crossborder transfer of data, and significant financial penalties for noncompliance.
>
> For example, failure to comply with the GDPR may lead to regulatory enforcement actions, which can result in monetary penalties of up to 4% of worldwide revenue, orders to discontinue certain data processing operations, civil lawsuits, or reputational damage. If any person, including any of our employees, negligently disregards or intentionally breaches our established controls with respect to client, third-party or Accenture data, or otherwise mismanages or misappropriates that data, we could be subject to significant litigation, monetary damages, regulatory enforcement actions, fines and/or criminal prosecution in one or more jurisdictions."

Lastly, Accenture confirms it has cyber insurance, but if it is under insured, the business could still face significant impacts from a cyberattack and the resulting litigation:

> "These monetary damages might not be subject to a contractual limit of liability or an exclusion of consequential or indirect damages and could be significant. In addition, our liability insurance, which includes cyber insurance, might not be sufficient in type or amount to cover us against claims related to security incidents, cyberattacks and other related incidents."

And that is the end of the section on cyber risk.

Did the report leave anything out? Would you or your organization say anything differently? Let us know in the comments below.

[Related Webcast] It's 2:00 AM, Do You Know Where Your Data Is?

Tags: Risk Management

Comments

First Name*

Last Name

Email*

Comment*

protected by reCAPTCHA
Privacy - Terms

Submit Comment

Email address*

SUBSCRIBE