Mergermarket
An Acuris company

TOPPAN
TOPPAN VINTAGE

The SEC Breach and the New Age of Cybersecurity

Data breaches dominated the headlines this fall, as credit agency Equifax and the Securities and Exchange Commission both suffered serious cyberattacks. In light of the hacks, the corporate world is grappling with how to protect itself.

The year 2017 has seen a paradoxical evolution in cybersecurity threats. On the one hand, large, shocking breaches seem to be on the rise, such as the Equifax intrusion that compromised 143 million Social Security numbers. Massive damages have also been seen at the likes of FedEx and container shipping firm Maersk, both of which said attacks by the NotPetya ransomware would cost them up to US$300m.

What's more, the SEC, which is itself responsible for disciplining companies for lax cybersecurity policies, had a high-profile breach of its own, calling into question the safety of filers' data.

At the same time, companies across industries are beginning to appreciate the impact of breaches and are taking steps to protect themselves. For example, the average cost of a data breach actually declined 10% in 2017 to US$3.62m, according to research by IBM and the Ponemon Institute. Nonetheless, the average size of a breach increased nominally by 1.8%.

What can companies do to improve their security further? And how should the SEC and filers react to the EDGAR breach? We spoke with six leading experts to find out.

Contents

The expanding threat

The experts

Jill Abitbol
Senior Editor, Cybersecurity Law Report

David Hickton
Founding Director, University of Pittsburgh Institute for Cyber Law, Policy, and Security

Ted Augustinos
Partner, Locke Lord

Devika Kornbacher
Partner, Vinson & Elkins

Michael Coden
Head of Cyber Security Practice, BCG Platinion (The Boston Consulting Group)

“We need to treat the threat as a systemic risk to our communications. We can take steps today to address it."

David Hickton, Founding director, University of Pittsburgh Institute for Cyber Law, Policy, and Security

Mergermarket **Data breaches such as that of Equifax have become increasingly common across sectors and geographies. Do you think hackers are becoming more sophisticated, or are companies' systems more vulnerable? Or both?**

D. Hickton, Pitt Cyber: It is always easier to play offense in this space than to play defense. That's part of the problem – purposeful, determined hacking will always have an advantage over a strong defense, because the environment is open by definition.

The second thing is that hackers are resilient. They adapt like a virus. You could see this in the cases I tried as US Attorney for the Western District of Pennsylvania: if you look at Evgeniy Bogachev, my indictment of him was for the Zeus 3.0 botnet, which means there were a couple of other versions before that. Zeus 1.0, for instance, was indicted in Nebraska in 2007.

So we need to treat the threat as a systemic risk to our communications. We can take steps today to address it, whether it's dual-factor authentication or segregating data or using encryption correctly. We need to look at the great work being done on security issues as well, such as the Cybersecurity Framework created by the National Institute of Standards and Technology (NIST) in 2013.

T. Augustinos, Locke Lord: I would say it's both – there's no question that the threat landscape continues to evolve with increasingly sophisticated attacks. While defensive technologies, strategies, and techniques are also developing, and more and more companies are improving their cybersecurity profiles, the increased connectivity of systems and availability of data does increase vulnerability.

In other words, more companies are getting better at cybersecurity; but even if they kept up with the developing threat environment, they would be increasingly vulnerable as a result of the growing connections at most companies among people, systems, and data. For example, companies are increasingly expanding their technology infrastructure by implementing connected devices, expanded remote access and internet capabilities, and new relationships with third-party service providers. All of these and more represent additional vulnerabilities.

D. Kornbacher, Vinson & Elkins: I would agree with Ted and say it's both things. As far as the vulnerability of company systems, more and more companies are using tools such as open-source software, which was the

point of vulnerability in the Equifax breach. As the use of open-source software and similar "open" tools increases, vulnerabilities will increase if a company is not diligent about installing updates and patches.

And as far as the sophistication of the parties that are doing the "hacking," I would say that even just five years ago, many cyber-attackers were just like common thieves. They would look for the door that was easiest to get into and go through that door. Their thinking was, "I'm going to attack points where there's not a lot of resistance." Now, there are people whose full-time job is to hack particular institutions.

And it's not, "[Knock knock] – oh wait, the door didn't open, let me go to the next door." It's, "[Knock knock – wiggle the door knob – try to get the hinges off] – okay, let's go get a battering ram." So I do think it's a combination of that increased vulnerability and the change in the mode of these cyber attackers that has allowed these huge breaches to occur.

M. Coden
BCG Platinion

Cybersecurity is a risk – it's not a whole lot different from the risk of an earthquake or some other natural disaster, or an epidemic. At a bank, for instance, they do credit risk analysis. And cyber risk needs to be elevated into that kind of business thinking; businesses have to make preparations. We conduct cyberattack simulations for companies as part of our consulting practice that are basically like fire drills.

There is a lot of confusion at many companies, because it was historically thought that cyber risk was an IT risk. It's only in the last year or two that it's really become obvious that this is an existential business risk. It's probably the one risk that can put an entire company out of business. Just in the last five months, hundreds of companies suffered billions of dollars in lost revenue when their entire operations were shut down by the WannaCry and NotPetya attacks. In 2012, a similar malware attack on Saudi Aramco destroyed an estimated 35,000 computers in 45 minutes. Too many companies thought "it could never happen to me." Now, five years later, it has.

There are very creative criminals out there who sell "malware as a service," complete with help desks and warranties. Moreover, billions of dollars are being spent by nation states on developing and stockpiling cyber weapons. It used to be that we had the navy for sea, the army for land, and the air force for air; then, space

became a military command. Now, in every major country's military system – Russia, China, the United States, Iran, and North Korea, as well as probably all our European allies – there is a cyber command with both offensive and defensive parts.

There is a fascinating issue that BCG is working on with the World Economic Forum about what the public-private partnership needs to be in cyberspace. For instance, if some nation state were to send an airplane over your factory and try to bomb it, the United States Air Force would shoot it down. But in cyberspace, it's just not that easy. We're trying to figure out how the government could help in equivalent situations like that.

Mergermarket **Given the frequency of data breaches, do you think they are becoming an inevitable part of the modern business environment? Should investors and the public be concerned every time one occurs?**

D. Hickton ⬣ Pitt Cyber I wouldn't panic about data breaches – panic is useless. But I would say there comes a point at which we have to resolve whether we have the will and the way to defend our data. If we're just going to accept that breaches are inevitable, then we're going to surrender our privacy, at least with regard to internet communications, and we're going to rely upon things being anonymous simply by virtue of the volume of the data. I don't recommend this.

I believe we've dealt with this before in human history. We've had these transitions, such as when we went from the telegraph to the telephone. But we have to be realistic about what the risk is; we have to be sober and purposeful about how we're going to deal with it; and we have to spend the money to take the steps necessary to address it.

We also need to come to a consensus about what we're going to require with regard to cybersecurity breaches. Are we going to require voluntary or compulsory reporting? What are we going do about information sharing? And most importantly, in the world of enforcement, are we going to update our tools, particularly mutual legal assistance treaties and extradition? Because this is a borderless threat, and we need to treat it as such.

D. Kornbacher ⬣ Vinson & Elkins This is a tough question. I would say the concern should not be overly focused on a particular breach but should be about what a company did or did not do in the preparedness area and how they're responding to the breach. If I'm

an investor, I'm much more concerned about those issues and that's what I want to uncover before I invest.

When I counsel companies in connection with due diligence for investments in tech companies, some of the points we spend a lot of time on are: What is the state of their information security program and systems? Do they have a business continuity plan with off-site back-ups? Have they been running tabletop exercises to practice their incident response plan? When was the last time they had a penetration test or an assessment done? And what were the results of that test?

A lot of times, cybersecurity risk assessments will uncover weaknesses. But if I see that the company has taken efforts to plug the holes, and is proactively trying to prevent breaches and has the plan to respond to them, then I'm much less concerned. I'm more concerned if I ask a company about their cybersecurity program, and they give me a piece of paper, but they don't have anybody responsible for implementing or overseeing the program. And if I ask when the last time it was that they looked at the program document, or practiced anything in it, or trained anybody on it, they can't say for sure.

T. Augustinos
Locke Lord

Cyber threats are here to stay, and compromises of data and systems have been an inevitable part of the modern business environment for some time. This is, as the SEC pointed out some time ago, a risk factor for most companies. The level of concern by investors and the public ought to be commensurate with the risk, and the SEC's disclosure guidance on this point was appropriate. It's not one-size-fits-all, and different companies and industries are more or less exposed than others. Prudent investors and members of the public should be considering their own cybersecurity profiles, and the profiles of the companies in which they invest or with which they engage.

Given the increase in the number and severity of reported attacks and breaches, there is a risk of desensitization, particularly among the general public. It's hard to stay vigilant but not overreact. In connection with some recent, high-profile breaches, we've started to hear, "Well, I'm sure my information is out there anyway." This presents a very real danger, given that we need constant vigilance at all levels of our economy and society, from individuals to companies to the government.

M. Coden
BCG Platinion

There's an equation that I think is useful in understanding cybersecurity risk.

The equation is: risk (R) equals threats (T) multiplied by your vulnerabilities (V) multiplied by the consequences (C). That is: R = T x V x C.

Now, the threats (T) are out there and there's nothing you can really do to eliminate them. They're coming from all over the place – nation states, political activists or “hactivists,” criminals, and anybody else. Previously, cybersecurity engineers thought, "Well, I can solve this problem. I can reduce my vulnerability (V) to zero." Going back to that equation, if you can make threats (T), vulnerabilities (V) or consequences (C) equal to zero, your risk (R) would go to zero. But now, companies are realizing that you can't drive those vulnerabilities to zero. It would require an infinite amount of money and time.

So, if you realize that you can’t reduce your vulnerabilities to zero, you have to begin focusing on the consequences. What can you do to minimize them? And what is the best way to allocate dollars to reduce your vulnerabilities to a reasonable amount? For example, if someone gets into one factory, or one part of your banking system, or one part of your enterprise resource planning (ERP) system, you want to prevent them from being able to traverse across and through your networks.

J. Abitbol
Cybersecurity Law Report

It is essentially an idiom in the industry at this point that it is not “if” but “when” a company will be a victim of a cyber event. Thus, we can’t emphasize the importance of incident preparedness enough. This includes having an effective incident response plan and testing that plan.

Equifax’s response to this incident may have been different had it tested its plan. It seems that if Equifax had correctly war-gamed a massive breach like this, these issues would likely have bubbled up.

An incident response plan with different scenarios should be tested regularly. Some of the experts with whom we spoke have suggested it should be tested at least once a year. All experts agree that a plan should not be tested for the first time in the midst of an incident, because mistakes can be made under pressure. If a company has walked through a plan in advance of a high-pressure situation, executing the plan will go much more smoothly.

It’s difficult to anticipate everything that can happen, because every breach is different. However, running incident scenarios against your actual inside response procedures is often enough.

EDGAR breached

The experts

Jill Abitbol
Senior Editor, Cybersecurity Law Report

Ted Augustinos
Partner, Locke Lord

Michael Coden
Head of Cyber Security Practice, BCG Platinion (The Boston Consulting Group)

David Hickton
Founding Director, University of Pittsburgh Institute for Cyber Law, Policy, and Security

Devika Kornbacher
Partner, Vinson & Elkins

“There is no way to totally protect any system. So, should filers be concerned? Yes, they should be."

Michael Coden, Head of Cyber Security Practice, BCG Platinion

Mergermarket **Do you think filers should be concerned about the security of the data they file with the SEC given the apparent cybersecurity vulnerabilities in the Commission’s systems? Are there ways for companies to protect themselves from the damage of potential future breaches?**

D. Hickton ⬣ Pitt Cyber Companies certainly can protect themselves better. And everyone is on notice right now that we're not only in the digital age – we're in the digital security age. Management teams need to do a better job of protecting their data and the infrastructure of their companies, as well as doing a better job of enforcing basic cyber hygiene by their employees. It's no longer just a mistake when someone doesn't use good cyber hygiene – it can cost millions or billions of dollars.

But when you talk about a system that is part of the SEC reporting protocol and is therefore outside the contours of companies’ individual systems, I think we have the right to expect better. I don't think we have to accept the Hobson's choice we're being presented with right now. Given the critical nature of the filing system and the fact that we've had signs of attacks before, I think we all have a right to expect more from the SEC. And I would be really disappointed if we didn't recognize at this point how exposed we are. So I would call upon those who operate in and around our critical infrastructure, and certainly our stock market qualifies, to up their game.

T. Augustinos ⬣ Locke Lord We now know there are and have been vulnerabilities in yet another environment. But to me, it’s just another environment – albeit an important one. Companies need to be working continuously to assess risk, and anticipate and address threats. Registrants don’t have the option of not filing with the SEC, just as individuals don’t have the option not to file with the IRS or to have their information provided to a credit bureau. Let’s stay highly focused on the data and systems within our control, and work to mitigate the risks to those data and systems.

M. Coden ⬣ BCG Platinion It's an interesting question. I would reiterate that there is no way to totally protect any system. I have a personal rule that I never put anything in an email that I wouldn't want to see on the front page of your publication. So, should filers be concerned? Yes, they should be concerned and careful about what they are putting in writing. Everyone should assume that there is some probability that anything in a digital format will be accessed by people you don't want to see it. There is no way to make that zero. We have a concept

“The EDGAR hack may make disclosing companies uneasy when they submit their filings."

Jill Abitbol, Senior Editor, Cybersecurity Law Report

we call “Protect the Crown Jewels.” All organizations need to prioritize the importance and value of their data and physical assets. You cannot protect all your assets equally, so focus resources on protecting those assets which are the crown jewels.

With the SEC and many other organizations, I think we do have a lot of issues with the systems being fairly old and no longer maintained by the original vendors. On the other hand, in some cases these systems are actually better protected than the newer modern ones. They're so old that nobody knows how to break into them!

Any modernization effort has to be done in a very careful way. We have a concept we talk about called designing cybersecurity into your systems. This means accounting for cyber in your systems from the very first design meeting – having cyber people there, making sure the networks are segmented, making sure there's two-factor authentication, making sure that the people processes and who's going to access the data is controlled, and so on and so forth. Doing that from the beginning, rather than adding it on at the end, is really what everyone needs to do. It will lead to a lower total cost of securing the enterprise and to much greater cyber resilience.

J. Abitbol
Cybersecurity Law Report

The SEC EDGAR hack is part of a larger trend of intrusions aimed at the transmission of financial information in both the public and private sector. Experts in the field with whom we spoke told us that they are seeing an explosion of criminals who are looking for weaknesses in the system of how financial information gets transmitted from companies to the public. The SEC as well as the FBI will need to figure out how to get ahead of this and be proactive in order to discourage this activity.

The EDGAR hack may make disclosing companies uneasy when they submit their filings. Companies must continue to comply with this requirement, but the SEC will have to earn back the trust of these companies. Some believe this should start with leading by example, such as by putting resources into building as impenetrable technological systems as possible.

To this end, Chairman Clayton has “launched initiatives to implement an internal cybersecurity risk profile and create a cybersecurity working group to coordinate information sharing, risk monitoring, and incident response efforts throughout the agency,” the SEC stated in a recent press release.

The SEC's tough road ahead

John Reed Stark

In August 2017, the Securities and Exchange Commission issued a "Risk Alert"[1] on cybersecurity that described the results of a recent examination of 75 companies' security frameworks. The findings struck a note of optimism, saying that nearly all the examined companies maintained written cybersecurity-related policies and procedures.

However, the document also said the firms "did not appear to adhere to or enforce [the] policies and procedures." In other words: the firms mostly had cybersecurity frameworks on paper only.

Just over a month after that "Risk Alert" was released, news broke that the SEC may have been guilty of this same error. Despite the SEC's increased emphasis on cybersecurity at filers in recent years, the Commission announced that its own EDGAR system was breached in 2016. What's more, the SEC delayed making the intrusion public until September 2017, and only in October did Chairman Jay Clayton reveal that the data in an EDGAR test filing also included the Social Security numbers of two individuals.

To be sure, most cybersecurity experts agree that data breaches are difficult to prevent altogether in the modern world – including at the SEC. But can the Commission maintain robust response procedures going forward? And should companies be concerned about the security of their filings in light of the breach?

Unique challenges

John Reed Stark, who served as the chief of the SEC's Office of Internet Enforcement for 11 years until 2009, said the Commission must cope with the same issues as corporations across sectors and geographies for the most part. "The challenges the SEC is facing in the area of cybersecurity are really no different than what every company doing any kind of business over the internet is facing," he said.

Nonetheless, he said, one area in which it has a disadvantage is obtaining funding – especially for high-quality employees.

"The only way to have really good policies, practices, and procedures is to have really good people, and there's a real crisis in the country right now with respect to cybersecurity professionals," said Mr. Stark, who now leads his own cybersecurity consulting firm. "There's such a small number of them. And major technology companies who are hiring can pay anybody working at the SEC twice or three times as much as they're receiving at the agency."

Upgrading hardware can be a challenge for the government as well. For example, after the SEC breach came to light, it was reported that the Commission's forensic unit had been forced to use outdated equipment that had been previously slated for disposal.[2] "There is a lot of pressure in government contracting to just take the lowest bidder, which I think is penny wise and pound foolish," Mr. Stark said.

1 https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

What's next

In response to the breach, the SEC has taken several steps meant to bolster its data security efforts. On September 25, it announced the creation of two new divisions tasked with addressing threats: the Cyber Unit, which will have a broad remit that includes responding to cyberattacks on critical infrastructure; and a Retail Strategy Task Force, whose focus is on protecting retail investors. The Cyber Unit is a revived version of the Office of Internet Enforcement, which was shut down in 2010 as part of an agency reorganization.

In addition, SEC Chairman Jay Clayton said in late September that he plans to request a boost to the agency's US$1.6bn budget from Congress to help cover additional security costs.

Perhaps the biggest concern of investors for the immediate future is the SEC's planned database of investor information known as the Consolidated Audit Trail (CAT), which is designed to help the Commission monitor markets better. In the wake of the EDGAR breach, lawmakers and brokers raised the idea of delaying the November 15 deadline for stock exchange operators to start sending data to the system.

2 https://www.wsj.com/articles/hypocrisy-and-hacking-1507330692
3 https://www.sec.gov/news/press-release/2017-176
4 https://www.washingtonpost.com/business/economy/sec-ignored-years-of-warnings-about-cybersecurity-before-massive-breach/2017/10/24/7e7507d0-adf7-11e7-be94-fabb0f1e9ffb_story.html?hpid=hp_hp-top-table-main_secbreach-230pm%3Ahomepage%2Fstory&utm_term=.4e6f5f1a2e78

The contractor responsible for building it, however, has said security is a foremost priority, and has warned against the consequences of halting data collection altogether. “The negative of the fear around cybersecurity is that if it’s used to kill every initiative that might involve gathering more data, then society loses,” Thesys Technologies CEO Mike Beller told Bloomberg in an interview in October.[5]

Assigning blame

The damage done in a cyberattack can be enormous – potentially even larger than the fraud perpetrated at companies such as Enron and WorldCom, according to Mr. Stark. The CAT system, for instance, could eventually contain personal data of more than 100 million trading accounts.

But at the same time, Mr. Stark warns against vilifying the victims of breaches, and contrasts them with embezzlers and fraudsters. “Senator Charles Schumer said that the incident at Equifax was the worst case of corporate malfeasance since Enron,” Mr. Stark said. “That's not just hyperbole – that's absurdity.”

“Because at Equifax, no one has been accused of trying to steal millions of dollars from the company,” he said. “At worst, the executives just didn't take security as seriously as they should have. But that's a far cry from the crooks of Enron who schemed to steal money from shareholders and manipulate stock markets.”

The estimated industry cost of reporting to the Consolidated Audit Trail is $1.7 billion

PwC 2016 report on the SEC's plan for the CAT system

5 https://www.bloomberg.com/news/articles/2017-10-10/audit-trail-could-boost-hack-risk-for-exchanges-executives-say

TOPPAN
TOPPAN VINTAGE

Capital Markets

EMPOWERED CLIENT SERVICE

At Toppan Vintage, we take pride in our mission to deliver a hassle-free experience with the highest quality, accuracy, reliability and value in financial printing. We have the scale, financial strength, conference and printing facilities, and team experience to handle any deal, any size.

We Understand

the dynamics of deals and know how to work with issuers, buyers, sellers, and legal and financial advisors.

RELIABLE SOLUTIONS:

- IntraLinks® Virtual Data Rooms
- EDGAR
- XBRL (Full-service & SaaS)
- Typesetting (The industry's only auto-pagination platform)
- Print
- Document production

CHANGE YOUR EXPERIENCE of Financial Communications

Hassle-free ⬣ Speed to Market ⬣ Innovative Technology ⬣ for all document, communications and filing solutions

Features and Benefits

of Toppan Vintage's Capital Markets Services

- High quality
- Reliable and accurate financial print services
- 24/7 support
- Experienced team with over 2 decades of industry experience
- Unparalleled technology solutions
- Streamlined process for cost savings
- Direct communication which simplifies work
- Company-owned conference, printing and mailing facilities
- Boutique experience for clients—working the way they want to work
- Strong financial backing (part of the world's largest printing and communications group)

KEY DIFFERENTIATORS

- Client-centric organization
- Working the way the clients want to work
- First-class technology
- Experienced team
- No hassle

KEY DEALS

- IPO and equity offerings
- Private placements
- Mergers and acquisitions
- Bank conversions
- Bankruptcy and restructuring
- Public and private bond offerings
- Securitizations

TOPPAN
TOPPAN VINTAGE

www.toppanvintage.com | marketing@toppanvintage.com | 747 Third Avenue, 7th floor, New York, NY 10017

About Toppan Vintage

WHO WE ARE

Toppan Vintage is a leading international financial printing, communications and technology company dedicated to delivering a hassle-free experience with the highest quality accuracy, reliability and value for your organization's financial printing and communications needs. Toppan Vintage is part of the Toppan Printing Group, the world's largest printing group, headquartered in Tokyo with approximately US$13 billion in annual sales.

WHAT WE DO AND WHY WE'RE DIFFERENT

Toppan Vintage provides software and services to handle mission-critical content that enables our clients to communicate more effectively and efficiently. We provide these services for capital markets transactions, financial reporting and regulatory compliance filings, investment companies and insurance providers.

The Toppan Vintage difference is simple – we are uniquely focused on the development and implementation of exceptional technology solutions, such as our Hive® suite of proprietary services, providing our clients with a competitive advantage when it comes to their financial communications needs. Despite our vast global reach, we're proud to offer boutique-like services allowing our team of experts to work hand-in-hand with our clients.

www.toppanvintage.com

For More Information
Sarah Reilly
Marketing Manager
Toppan Vintage
201-562-1798 | sarahreilly@toppanvintage.com