CISOs' LESSONS from Security Breaches

Insights from 5 cybersecurity leaders who have guided teams through severe security breaches.

Written by: Julian Brown

LUMU

Index

Executive Report

Preparation Is Everything

Michael Coates - Former CISO at Twitter

Coates shares how preparation is invaluable to ensure that a security breach is not a failure. Sufficient preparation will avoid an egregious catastrophe.

KEY LESSONS

- *A Breach Doesn't (Always) Mean Failure*
- *Build a Reliable Team*
- *Invest in Investigation*

Don't Underestimate the Ruthlessness of the Adversary

Rafaela França - Former Head of Information Security at Mater Dei Hospital

França's team was already fighting to deliver IT access to doctors serving 20,000 patients per day at the height of the Covid 19 pandemic. Then a ransomware attack struck.

KEY LESSONS

- *Create Strategies with Redundancies—on All Fronts*
- *Establish Systematic Monitoring*
- *The Adversary is Ruthless*

Communicating with Respect

Tim Brown - Current CISO at SolarWinds

The Sunburst attack on SolarWinds brought the term 'Supply chain attack' to the forefront of cybersecurity. Tim Brown reflects on the importance and challenge of clear communication throughout.

KEY LESSONS

- *Communicate with Transparency*
- *Focus on the Customer*
- *Assume Breach*

Be Humble

Márcio Sá - Former Head of Information Security at Localiza

Sá looks at the sheer scope of the challenge posed by a massive breach and where to turn to for assistance.

KEY LESSONS

- *Trust (and Where to Place It)*
- *Use All Your Tooling Fully*
- *Humility*

Notice the Patterns

Bret Hartman - Former CTO at RSA

Technologist Hartman considers the lessons from the 2011 RSA breach—the paragon of all supply chain attacks. A decade later, have those lessons been learned, and are we any better off?

KEY LESSONS

- *Visibility is Always Key*
- *Have a True Understanding of Risk*
- *Notice the Patterns and Act on them*

Michael Coates

Former CISO - **Mozilla and Twitter**
Founder - **Altitude Networks**
Current CISO - **CoinList**

Preparation Is Everything

The Incident

For Michael Coates, two interesting incidents come to mind from his time at Twitter. The first was a nation-state attack perpetrated by Saudi Arabia coordinating with insider employees. “That was a worst-case scenario, with well-funded adversaries and insiders—really all the challenges that come to mind,” remembers Coates.

On the other hand, there was another purported breach where attackers reported to journalists that they had access to millions of user names and passwords. Ultimately, it turned out to be a false claim, but it still had to go through incident response procedures.

> *“That was a worst-case scenario, with well-funded adversaries and insiders—really all the challenges that come to mind”*

The bad news can come through different channels. “In all those situations your heart stops and there’s a bit of panic,” remembers Coates. “You immediately start thinking about gathering information to prove, disprove, or investigate further. Who do we bring into the room? What systems will we need?”

Ideally, you should be thinking about the preparation you’ve already executed. The runbooks and playbooks. Tactically, it’s also a time to clear the calendars, get all hands on deck, and get ready for some late nights.

The Lessons

A Breach Doesn't Mean Failure

Some see security as a team that is intended to prevent all breaches. Coates disagrees, somewhat. If a security team is given the goal of preventing all breaches, then they would crush all risks at all times. This would nullify any business decision that could intrude risk. That would be a silly way to do business. On the other hand, customers expect you to protect their data.

"A data breach doesn't necessarily mean failure, but that's with a very big asterisk," says Coates. "What matters is how bad the breach is and how much you prepared ahead of time."

There's a limit to how much a company can prepare. It's possible for a company to do everything humanly possible while operating all the latest cybersecurity tools and a breach can still happen.

The expectation is that

- You have implemented all industry-standard security controls.
- You have planned and prepped for a breach.
- When a breach happens that you will be forthright and public about what you know and don't know.
- Because you have mitigating controls, the breach will not be catastrophic.

> *"A data breach doesn't necessarily mean failure, but that's with a very big asterisk"*

"What consumers, businesses, and the public at large won't be understanding of is if the breach is egregious, says Coates. "Then, I do think a data breach could mean failure."

You'll Learn More About Your Team

"You definitely see who's ready to operate under pressure," says Coates. "One thing that Hollywood gets right is the image of peo-

> *"If you've built a good, solid team ahead of time, that will pay off dividends extensively in situations where they need to shine"*

ple hunched over laptops surrounded by pizza boxes. You're all working together until after you thought you would go home and until the brain cells stop working."

You'll also see who's able to problem solve creatively, whether that's in connecting the dots or working around when a data set isn't perfectly formatted.

You'll see who's able to think like an attacker. Psychology and motivation start to play a role. There are a lot of things that could happen, but the question is what did the attacker do? You'll notice who are the people who can adopt that detective mindset.

Another characteristic is '***organization under disarray***'. Some people are able to take disparate data and formulate it into a precise report of what happened. They are able to form timelines and acknowledge where the gaps are, so that those gaps can form lines of inquiry.

"If you've built a good, solid team ahead of time, that will pay off dividends extensively in situations where they need to shine," advises Coates

Don't Try to Hire 'Unicorns'

"Some of the best security engineers and analysts I've worked with had varied and unique backgrounds" recalls Coates. Many people that thrive during a severe breach are people who have in the past been placed in stressful situations—and not necessarily related to technology.

One person Coates worked with had previous experience as a coordinator of farmhands. This lent them management skills and an invaluable figure-it-out mentality. Another person had experience as an EMT dealing with high-stress medical emergencies.

> *"At the end of the day, you want all your information in a single place where it's easy to query and cross-reference"*

"The 'talent shortage concern' is a reflection of the immaturity of the industry," says Coates. "Far too many security managers are hiring what I would call unicorns." Some job descriptions in the cybersecurity industry are unrealistic, requiring 10 or 15 years of job experience. These descriptions are too senior and overlap disciplines.

Cybersecurity leaders need to go over their teams and break down roles into distinct levels. You should have distinct senior roles and also pull out junior tasks for up-and-coming new talent. A pipeline can be formed with those new junior roles. "At Mozilla and Twitter we had a wonderful pipeline of junior talent and internships through Year Up." says Coates. "So, I don't know if I buy 'the shortage'. I think a lot of that falls on us."

Invest in Investigation Tools

A lot of the work and time is centered on investigation. You're trying to collect all the information and figure out the attackers' trail. That information is shaped into a concise statement of facts.

"At the end of the day, you want all your information in a single place where it's easy to query and cross-reference," says Coates. You can have a large array of tools at your disposal, but while it might sound simple, getting the right data at your fingertips with cross-referencing is hard to achieve.

Leverage computers working for you by automating repetitive tasks. You don't need to reinvent the wheel every time you need to do something. Reserve humans for problems that are so hard that they need human thought.

The Breach Experience Is Grounding

Experiencing a breach first-hand shows you what you are trying to prevent in the first place. "A lot of security is hand-wavy embel-

lishment—and it shouldn't be," says Coates. The motivations in the cybersecurity industry are unfortunately driven by checkbox compliance. Security for compliance is very different from security for not getting breached. Be compliant—but that's not where you stop by any means.

For example, you can do encryption of at-rest data in your cloud instances for the purposes of compliance. But you'll start asking yourself, "how does that protect me when the data is constantly in motion and the attacker would come through the application anyways?" Your thinking will start to focus more on how the attackers are actually operating and what would stop them. Going through a data breach makes it all very real.

Preparation Is Everything

"When you go through a breach, you'll start to think about all the things you'd wish you had done before," says Coates. "You'll say that I wish I had these things lined up, those tools ready, and all these playbooks prepared. ***So, do those things now***."

In his first few months at Twitter, Coates set up a breach simulation. They had a controlled 'external' party claim that they have access to confidential data. They watched how the PR, legal, and security departments responded. In this controlled environment, they could see what worked, what didn't work, and make a number of changes.

Create the breach now through table tops or through simulated breaches. Watch how your team responds and where things fall apart. That way you can know the things you would have wished you'd known, before a breach really happens.

"Leverage that 20-20 hindsight, before it becomes hindsight," advises Coates.

> *"When you go through a breach, you'll start to think about all the things you'd wish you had done before"*

Rafaela França

Founder - **IT Advisory**
Co-founder - **Ctrl Saúde**
Former Head of Information Security - **Mater Dei Hospital**

Don't Underestimate the Ruthlessness of the Adversary

"The cybersecurity space is a cold war, where adversaries wield inexpensive weapons that cause massive damage." says Rafaela França. "It has accelerated around the world, becoming more complex and more difficult for its defenders."

The Incident

During the height of the COVID-19 pandemic, Rafaela França was in charge of IT at a large Brazilian healthcare group. They were already in crisis mode to coordinate service delivery amid the deepening national and global emergency. The day before a national holiday, they saw the message 'Your data is encrypted. To access it contact prontoemail.com.' It was a severe ransomware attack originating from China.

> *"What started with a compromised medical imaging and diagnostics tool resulted in 90 days of intense instability"*

Suddenly, 2,500 computers and 350 servers were down. 200 integrated systems were unavailable. Critical services were unavailable to 3,000 employees and 5,000 healthcare professionals including doctors who saw over 20,000 patients per day.

"It was a nightmare; there was total chaos," remembers França. 100% of their processes had to migrate to manual, pen-and-paper processes. Across the organization, employees, doctors, and leaders experienced extreme stress and sleepless nights over an extended period of time while they addressed the crisis.

> *"What started with a compromised medical imaging and diagnostics tool resulted in 90 days of intense instability"*

They immediately activated their contingency plans. França led 500 technology experts in a war room with 24/7 operation over 90 days. They had to establish direct and fluid lines of communication with over 120 leaders and 25 partner companies, including crisis management consultants.

Unfortunately, the response team could not limit the perimeter of the attack. They were, however, able to reset all devices, build an authenticated network, and restore backups to get critical systems running again. "What started with a compromised medical imaging and diagnostics tool resulted in 90 days of intense instability—and I cannot overstate this enough—a massive challenge," says França.

The Lessons

According to França, the key to success is to prioritize the security incident and implement continuous improvements.

Develop an Attack/Defense Map

Understanding your opponent is key to winning. To develop an attack/defense map with threat modeling, you will need to first understand the adversary's tactics and strategies. You can then create a map that will help you visualize the battlefield, and allow you to develop specific strategies to counter the adversary's moves.

Create Strategies with Redundancies—on All Fronts

You can't be too careful when it comes to preparing for a security incident. You must have backups of your data, staff, and plans in place so that if something does go wrong you will still be able to

recover from the situation quickly with these resources at hand. It's also important that we not only monitor ourselves but make sure our system is monitoring itself as well—this way any threats detected early on won't cause major issues down the line.

Establish Systematic Monitoring

One of the best ways to protect your organization from cyberattacks is by establishing systematic monitoring, which is supported by different players who will audit each other. By doing this, you will be able to detect any threats as soon as they occur and respond quickly and effectively.

However, in order for this system to work effectively, it is important that all players are working together and are aware of their roles in the system. Furthermore, you need to make sure that the system is constantly updated with the latest information so that it can be effective in detecting any new threats.

The Adversary Is Ruthless

The adversaries we face will always strike when we're most vulnerable. There's no room for compassion. In this case, França's team was at the height of a health emergency and working to deliver critical services to extremely vulnerable people. None of this matters to the adversary. If anything, it just increases their avarice and attracts them like sharks tasting blood in the water.

"The adversaries we face will always strike when we're most vulnerable"

Have your contingency plans ready. Have strategies with redundancies, systemic monitoring, and an attack/defense map in place. Be prepared to execute your contingency plan and enter 'war room' mode. But most importantly, remember the compassionless nature of the adversary we face. Remember how ruthlessly they will exploit any opportunity they find.

Tim Brown

CISO - **SolarWinds**

Communicating with Respect

The Incident

On Saturday morning, December 20, 2020, Mandiant contacted SolarWinds, telling CISO Tim Brown that they had discovered something. Mandiant CTO Charles Charmakal laid out the details. It was SolarWinds' worst nightmare: they had shipped tampered code.

"At that moment, you don't have the luxury of thinking about yourself or your experience of the moment," says Tim Brown. The SolarWinds team's first actions were to get the right people on board and to establish and verify the facts. Luckily, Mandiant gave enough information to know that the threat was real very quickly.

"This attack wasn't just about SolarWinds. My Christmas and New Year's days were ruined, but so many of our customers' Christmases and New years were ruined as well," recalls Brown. Those customers included federal agencies like the CDC, most fortune 500 companies, and government contractors like Lockheed Martin.

"My Christmas and New Year's days were ruined, but so many of our customers' Christmases and New years were ruined as well"

The Initial Communications

In the first days, the SolarWinds team focused on piecing together all the knowns and unknowns so they could issue a statement. Less than 2 days later, around 2 AM on Monday, they finalized our first official response, before the opening of the stock exchange.

> *"You don't just have customers calling you, you have countries calling you"*

At that point, the incident response team already knew a lot about the incident. They knew that 18,000 accounts had downloaded the product. Among those, it turned out that the number that led to a secondary attack was under a hundred. But at that point in time, they disclosed the highest possible number that they could have, out of an abundance of caution. They knew that it was a sophisticated attack, that it did not affect their source code, and it had to come from somewhere in the build process. So, by day two, they knew it was a supply chain attack.

The Lessons

Be Prepared for Long Days

"People often ask why you're so busy and why you're all in that war room until 2 in the morning." says Brown. At 9 pm everyone would come together to get status updates on all the day's 'streams of work'. At 10 pm the board would convene for daily updates.

"You don't just have customers calling you, ***you have countries calling you***," stresses Brown. Government agencies and special projects called. For example, Project Warpspeed was underway at the time to support the development of covid vaccines. They were concerned that anyone who was working on the vaccine was on the list of affected customers. The FBI sent questions. CISA was in constant communication to develop recommendations.

Those are the types of questions received and for every question, the response needs to be reviewed by Brown—as the CISO—and by legal partners in very fine detail. The review process would

usually start at 11 at night. There's so much that needs to get done that your first month is spent in controlled chaos.

Bring in the Right Partners

Don't try to go on your own. In an extraordinary breach, it's crucial to bring in people who have experienced similarly extraordinary incidents and have the right context. DLA Piper helped SolarWinds with FBI contacts. Former CISA director Chris Krebs helped them get in touch with all of the national defenders of the world. Alex Stamos brought in some of his corporate cybersecurity experience. Bring the right folks in that can help you facilitate that kind of major incident response.

"The first couple of days are incredibly hectic and you're scrambling to get everything done and bring in the right people," remembers Brown. "There are a lot of streams of work that need to be coordinated. You must explore what happened in your IT, Engineering, Security, and Communications departments."

"The first couple of days are incredibly hectic and you're scrambling to get everything done and bring in the right people,"

Externally, SolarWinds got DLA Piper as their legal partner. They had a threat-hunting partner in Crowdstike. KPMG's forensics team was brought in to investigate the development and engineering streams. DLA Piper ended up helping a lot to 'quarterback' and coordinate different streams of work, including with other 'minor' partners.

Communicate with Transparency

The more you communicate at the beginning and the more you communicate openly with your customers, the better. Being the face of a breach of this scale and answering calls from the coun-

tries of the world requires a very different skill set than what most CISOs' are accustomed to.

Focus on the Customer

"There are a large number of agendas running amock in a large incident like this—that was something I didn't expect," recalls Brown. "If we had focused on addressing all the misinformation in the press, we would still be doing that today."

For example, the press caused confusion by talking about the 'SolarWinds breach' or 'SolarWinds attacks' in connection with companies that didn't have any SolarWinds products. What they meant to say was that the same entity was responsible for those attacks. You have to accept that the press is going to go wild and won't be well-informed. If you have a cool-sounding or trending name it will be used against you.

"If we couldn't talk to the press, ex-employees or researchers we'd worked with years before would talk to them, spreading rumors and misinformation. It is impossible to answer all of those questions coming from the press," says Brown.

Instead, focus on the customers' questions like 'How do I know if I am affected and what do I do if I am affected?' CISA proved to be a great partner in helping to amplify the truth and give companies guidance.

"Treat the incident with respect. Respect your partners. Most importantly, treat your customers with respect"

Assume Breach

The SolarWinds team understood that in overcoming this breach they couldn't just be 'okay'. They needed to be exemplary. "Our build environments relied on a lot of infrastructure to protect things from getting corrupted," says Brown. SolarWinds had a

> *"You can share and be transparent enough to help people without destroying a company"*

resilient model from an access perspective, but it didn't have a true 'assume breach' model. Their newer model has a true 'assume breach' perspective. They always had peer review, but now there's an architecture review as well.

As part of 'secure by design', SolarWinds now has triple checks, so you would need collusion on a whole different level to get breached. Some would say that's overkill, but they say that's part of being exemplary. "There's always some risk in control design, but what we've done is make it much, much more difficult and expensive to get around those controls—and we've done that across the whole organization."

Personal Growth

"Going through this type of severe breach gives you a better understanding of the pieces involved." says Brown. "You understand the different approaches involved. It shows that you can be humble, open, and honest. You can share and be transparent enough to help people without destroying a company."

"Being one of the public faces of an event like this makes you grow as a person. You connect with and talk to thousands of affected people from across the world. As much as it is a negative experience, it's something you can grow from and give a little back to help the world and the industry."

"Treat the incident with respect. Respect your partners. Most importantly, treat your customers with respect," concludes Brown.

Márcio Sá

Founder and Security Strategist - **Castle Security Services**
Former CISO - **2TM Group**
Former Head of Information Security - **Localiza Rent a Car**

Be Humble

The Incident

It started with a message on Whatsapp. Certain systems were reported to be behaving strangely. Then Head of Information Security Márcio Sá decided to investigate with the IT team. After analyzing what seemed like just another unavailability case, it turned out to be a ransomware attack. Sá remembers finding the ransom note on the servers, putting his hands on his head, and saying "Oh my gosh, this is a terrible situation."

They immediately created their war room, notifying the VP of Technology, convening partners, IT staff, and cybersecurity specialists in one physical room. "I was in that room from Sunday afternoon and I left it Wednesday night. During those 4 days, I only slept 6 hours," recalls Sá.

> *"I was in that room from Sunday afternoon and I left it Wednesday night. During those 4 days, I only slept 6 hours"*

The Lessons

One Person Can't Coordinate Everything

The first big lesson was that it is impossible for one person to coordinate everything and everyone in that war room, especially with the pressure of the business being stopped. There was a cybersecurity crisis management plan in place, but the documentation was very recent and not communicated to the entire company. This kind of plan is necessary to organize and coordinate actions and connect the areas with the same goal. The crisis

scenario is more complex than one might imagine and there were too many things to do and dots to join for one person alone.

If you have cybersecurity insurance, it's critical to take notes on every meeting and every action that is taken. Document every responsible person and the communications that took place. Moreover, practice shows you other relevant aspects that are usually not written down anywhere. For instance, team feeding, analyst rotation (24/7), forensic containers, NDA agreements, photographing follow-up sessions, recording costs and all hours worked, and others. "My advice is to use a specialized company to communicate and orchestrate the crisis. The CISO needs to have a clear mind (even if it doesn't seem possible) to make correct decisions," says Sá.

Trust

"My advice is to use a specialized company to communicate and orchestrate the crisis. The CISO needs to have a clear mind (even if it doesn't seem possible) to make correct decision"

The internal team learned a lot about trust from working closely during the incident. Realizing that the whole team is in the same boat made a big difference in their team spirit, cooperation, and willingness to put in the extra hours to overcome the incident.

By contrast, Sá was disappointed with some of his external security partners. "It's usually expected that super experts will come to help solve the problem and that's not what happened," said Sá "In addition to the questionable technical quality, some were slow in responding and didn't have the same sense of urgency, which created a lot of problems. Using SaaS tools is good for optimizing cost and time, but where is your data when you really need it? And does your team know how to fully operate the contracted tools?"

Another big lesson was that you need trustworthy partners. And

> *"Many cybersecurity leaders invest in the latest tools but don't use them fully or don't have the human resources to use them correctly"*

obviously, do not create dependencies (lock-in) with third parties, both in services and tools. "As much as you need internal and external partners, the responsibility always lies on you as the CISO," says Sá. "It's your responsibility to ensure that those reliable partnerships are in place. It's your responsibility to ensure that your team has a domain about all technical resources."

Use All Your Tooling Fully

The adversary usually has the advantage. That's generally true in security, but especially so during a breach. Firstly, they have the advantage of time, so you are always playing catch up. Secondly, they have the advantage of a large number of distribution points they can attack while you have limited resources to defend them.

You need to extract every advantage and that means using every part of every tool that you have. "Don't build your house from the roof down," says Sá. Many cybersecurity leaders invest in the latest tools but don't use them fully or don't have the human resources to use them correctly. Instead, focus on the basics and add proven cybersecurity capabilities that can be used fully. This also preserves the company's investments and demonstrates the maturity of security leadership in the execution of the security program.

Be Proactive

"Proactive actions are the most important," advises Sá. "Planning, planning, planning, and then testing those plans." These plans and playbooks need to be in place well before the incident happens and continually tested to ensure that they are up to date. Make sure that those plans are communicated across the whole

company so that every party knows what their responsibilities are during a breach.

However, there will always be a difference between a drill and living through the real deal. Namely, communicating those plans to all the affected parties proved really challenging. For that reason, it's crucial to involve experienced professionals who have dealt with responding to similar situations.

Cybersecurity Is a Company-wide issue

Cyber Resilience is a corporate problem, not just a security team problem. Security is closely connected to risk, and risk is closely connected to the business itself. At many companies in Brazil and elsewhere, the head of security is not a C-level or upper management position. This can lead to mistaken thinking that security is only a problem for the security team.

Being cyber resilient is much more than just security procedures. It involves crisis management, disaster recovery, business continuity, backups, and others. Importantly, it requires buy-in from the highest level of the company. "The head of security should work together with the head of technology," says Sá.

For Sá, one of the outcomes after the breach was a set of updated playbooks that laid out the actions for the entire company to take under different scenarios. These new playbooks included the actions to be taken by the entire company and include various different eventualities in a flow-chart fashion (with practical lessons learned in the crisis).

"The head of security should work together with the head of technology"

Humility

Know your weaknesses and give visibility about them. You'll have

> *"Understand that you don't have full control and that the adversary has the advantage—in time and sometimes also in budget"*

to admit that your environment has vulnerabilities since the adversary has gained access in the first place and it will be impossible to fix everything alone.

The incident response team needs to know about the limitations you have. "Understand that you don't have full control and that the adversary has the advantage—in time and sometimes also in budget," says Sá. "Understand that you will have to present the business risks and ask for help on many fronts."

The CISOs' responsibility is bigger than others can imagine. There is a lot of stress that comes with that. "Professionally I understand more about people, partners, the position's responsibilities, and being strict when it comes to business risk. These questions make me a different professional after the incident," says Sá.

Bret Hartman

Cybersecurity Lecturer - **California Polytechnic State University**
Former VP & CTO - **Cisco**
Former CTO - **RSA**
Former CTO, Information Security **- EMC**

Notice the Patterns

The Incident

In 2011 RSA was one of the world's largest and most reputable information security providers. Their flagship product was SecureID, a physical token that provided two-factor authentication to over 30,000 customers. If you worked at an organization in 2011 that took its security seriously, the chances are good you had one in your pocket.

In the Spring of that year, nation-state adversaries gained access to RSA's systems and took off with one of their most critically valuable assets: the seed bank that SecureID used to generate authentication codes. In theory, the adversary could generate MFA tokens for any of SecureID's customers. The RSA breach was the first known massive supply chain attack and CTO Bret Hartman was closely involved in responding to the incident.

> *"We thought that was the end of RSA. We thought this was existential and that the company wouldn't survive"*

Hartman remembers when they first got the bad news. "We thought that was the end of RSA. We thought this was existential and that the company wouldn't survive," remembers Hartman. "To RSA as a security vendor, our reputation and the value of the product ***that we sold to 40 million users*** was completely in jeopardy. That was not a fun day."

The Lessons

Visibility Is Always Key

"Without visibility and monitoring, you won't know that something is wrong," says Hartman. "When something finally happens to reveal that there is a compromise, it might be too late."

Luckily, RSA had access to the best information security technology and talent in the world at that time. Today, the average breach remains undetected for 201 days. The RSA team managed to detect the breach within 5 days of their initial access.

Having thorough defensive capabilities and good cyber hygiene will always be important. "But it is impossible to have perfect hygiene," writes Hartman on his Medium blog. "You must assume that attackers (or insiders) will make it inside the organization to attempt to cause damage."

RSA's security tools and extensive application-level security allowed them to see in near-real time what the adversary was doing. At that stage, it was unclear what the threat actors' intentions were. Nevertheless, as soon as the adversaries jumped to a new asset or system, RSA's threat hunters were right on their heels.

"You must assume that attackers (or insiders) will make it inside the organization to attempt to cause damage"

As the breach was developing, the security team was relatively calm. There were indications that the threat actors could not access customer credit card details or other sensitive customer information. They were confident that the attackers would be kicked out before any damage could be done—until the SecureID seeds were stolen.

“Putting together a security system and controls is based on your perceived risk”

Investigate Quickly and Get Ahead of the Breach

Because of their early detection and monitoring, RSA’s incident response team was able to see the adversary’s intentions as soon as they became apparent. They found that the actors had siphoned off the seeds to a hacked server. They even managed to gain access to the server, but before the analysts could delete the stolen files from that server, they were ferreted away to an unknown location.

As much as the stolen seeds were a grave disappointment, the upshot was that RSA knew about the risk as soon as the attackers’ intentions became clear. They could then inform all of their customers about the threat and advise them on how to take mitigating actions.

“As far we know—although there is some debate on this point—the RSA breach never led to a secondary attack that exposed our customers’ data,” said Hartman. If RSA had taken the industry-average time to detect the breach and if they were not able to investigate quickly and stay toe-to-toe with the infiltrators, the story could have turned out very differently. The attackers could have been able to cause damage on a massive scale.

Have a True Understanding of Risk

“Putting together a security system and controls is based on your perceived risk,” says Hartman. “You have to measure risk and balance the countermeasures against that risk. In RSA’s case, we were primarily concerned about the risk of our intellectual property being stolen.”

What RSA didn't fully appreciate at that time was the risk to their customers. In aggregate, that was the greater risk. "It's extremely difficult to ascertain what the risk is of losing the blueprints to an F16 fighter jet," says Hartman. "RSA doesn't know anything about fighter jets." However, the attacker understood that the best way to get to the design drawings could be by subverting the authentication process.

Today, the world is far more interconnected than it was in 2011. It's no longer possible to only consider your own internal risk. It's critical to consider the risk that you are exposed to through the suppliers above you, as well as the risk that you expose to your customers.

Understanding your true risk—not just perceived risk—is much more difficult.

Don't Have Complete Trust

The fact that the most reputable software providers like RSA and SolarWinds can be the source of a supply chain attack should alert consumers to the danger of implicit trust.

Today, we have implicit trust in untold third parties: Zoom, Google, AWS, and many others. "The attacker could potentially subvert that trust in ways that we cannot even predict," says Hartman.

> *"The attacker could potentially subvert that trust in ways that we cannot even predict"*

One of the scary implications of the RSA breach lies in its brazenness. If the attackers could target and successfully breach RSA, what's to say that less well-defended suppliers haven't been compromised?

Organizations should interview their critical suppliers to make

> *"Have monitoring and visibility in place so that you can correctly measure your own risk"*

sure that they also have the necessary visibility capabilities as well as the ability to monitor and get ahead of a breach.

Act on the Patterns

"I have never been a Chief Information Security Officer," says Hartman. " My job has always been on the technology side of developing products to stop these sorts of breaches. My job as a technologist is to see the patterns and act on developing solutions."

"The RSA breach of 2011 was the canary in the coal mine—a pretty big canary," says Hartman. "Now, it's a hundred times worse. Think about the integrations and dependencies we have now." And yet, we aren't much better off than we were then.

There's no one easy answer to the question of mitigating supply chain risk. You can minimize the number of suppliers you have. Don't have implicit trust in your suppliers or defenses. "Be Paranoid," advises Hartman. "Have monitoring and visibility in place so that you can correctly measure your own risk. Have a plan in place to recover when something goes wrong." For now, it seems that supply chain risk is something we all have to live with.

In the end, Hartman concludes that we need to focus on learning and continuous, incremental improvement. "What can we learn from these breaches so that we can stop them or mitigate them for many organizations?"

www.lumu.io

Lumu Technologies Inc. | 8600 NW 36th Street, Suite 150 Doral, FL 33166 | info@lumu.io | +1 (877) 909-5868