SpyCloud

Surviving a Data Breach

Security Leaders Offer Real-World Advice for Stronger Breach Prevention and Response

> “
>
> ***No company wants to go through this*** *but we’re seeing attacks continue and – everybody’s realizing that it’s not a matter of if, just when — and any organization could be targeted.*
>
> - Roy Mellinger,
> Former CISO of Anthem

If 2020 taught us anything, it’s the importance of preparedness. The common refrain, ‘it’s not a matter of if your company will be breached, but when’ is even more true today.

Large-scale data breaches spiked more than 270 percent in 2020, costing companies billions as criminals take advantage of the massive increase in business conducted online. The average cost of a data breach is now a staggering $3.86 million, with healthcare breaches costing an all-time high $7.13 million.

So to help your company survive a data breach, SpyCloud recently sat down with three seasoned CxOs – two from the healthcare industry and one from hospitality – who successfully led through worst-case scenarios: breaches that exposed customer data.

Through this candid exploration, each executive offers lessons they learned at every step that are relevant to security leaders from all industries, including:

- What fundamental security tools and procedures every company should already have in place
- How the breaches were detected
- How they communicated with company leadership, boards of directors, the media, regulators, and customers
- How they navigated litigation
- What types of long-term security investments they made post-breach, and how they sold those changes to leadership

This rare peek from the C-suite into the full lifecycle of real-world data breaches can help you better prepare your own prevention and response plans. First, let’s meet the three executives who shared their time and lessons learned.

Meet the Executives / Breach Overviews

Roy Mellinger serves as Managing Partner of The Shield Group, leading its cybersecurity consulting practice, which is focused on helping organizations improve their cybersecurity, breach mitigation and incident response programs. He has more than three decades of success developing and building industry leading information security, data protection and technology risk management programs from companies including GE, Sallie Mae and Sabre.

In 2015, Roy was serving as Chief Information Security Officer for Anthem, the largest health insurance company in the U.S., when a Chinese hacking group stole the sensitive data of 78.8 million customers and employees, including names, dates of birth, addresses, telephone numbers, email addresses, income data and social security numbers. By the time the dust settled in 2017, Anthem had paid $115 million to settle a class action lawsuit — at the time, the largest data breach settlement in history with the most health records stolen. Yet its response can be held up as one to emulate, with plans in place that allowed the company to, as Roy put it, "row the boat in the same direction to get through it; not only to resolve the breach but to deal with the court of public opinion, the political aspects and the litigations that were soon to follow."

Harry D. Fox is currently a Principal at Oak Advisor's Group, a strategic advisory firm focusing on the intersection of information technology and healthcare. From 2011-2018, he served as Executive Vice President, Chief Information Officer and Shared Services Executive at CareFirst, a $9 billion not-for-profit health care company offering health insurance products and administrative services to more than three million individuals and groups in Maryland, Washington DC and Virginia. Harry has also held senior-level positions at Kaiser Permanente, Coventry Health Care (now Aetna), and PwC, and serves on the boards of multiple private equity-backed companies and not-for-profit organizations.

While serving as CIO at CareFirst, Harry dealt with a 2014 breach that affected 1.1 million customers, stemming from a phishing incident with the same digital signature as the attackers who compromised Anthem. CareFirst was relatively lucky in that the data stolen did not include social security numbers, credit card data or medical information, but it still exposed names, addresses, dates of birth and member IDs.

Damian Taylor is a computer science and information security expert, a retired U.S. Naval Officer, and currently serves as the Senior IT Specialist for the United States Postal Service Office of the Inspector General. During his 20+ year career, Damian has served in multiple IT security roles within the Department of Defense with a focus on national security, information privacy, computer network defense, penetration testing, compliance, cybersecurity policy and strategy development.

When Damian became CISO of Landry's, whose 60 brands include restaurants, hotels and casinos, online gaming and the Houston Rockets, the company learned of a breach that exposed credit card data used at 46 of those brands, across 350 locations.

We recorded our interview with Harry and Damian for a live webinar, which you can watch on-demand here; we sat down separately with Roy. All three interviews have been edited for clarity and length.

Pre-Breach Fundamentals

All three executives agreed, if your company hasn't been breached – yet – your first priority is to focus on security fundamentals, which break down roughly along three tracks: your human risks, your infrastructure risks, and your third-party risks. Roy noted that many attacks are opportunistic so it's key to check that your basic blocking-and-tackling mechanisms are in place.

> **Roy:** I liken it to physical security. Somebody's walking up and down the block checking door knobs, or walking through a parking lot checking door handles. If your home is locked up, your car is locked up, you've prevented yourself from becoming a victim. The bad actor's going to move on to the next house or next car. But, if your basic network isn't secure, if you haven't done the fundamentals, then right off the bat, they found an easy target.

These fundamentals include:

- Do you have a patch management process in place, and are you patching in a timely manner?
- Are you doing vulnerability scans regularly, not just once a year or every 6 months?
- Are you just scanning the DMZ or are you also scanning customer-facing applications?
- Are you doing code scans of your apps?
- Are you scanning internal servers, databases, and endpoints? Constantly, and not just once a quarter or once a month?
- Do you have a server-hardening approach or program where you can guarantee that every server has the right security tools in place, is patched, etc? Is somebody auditing that?
- Are admins using secure passwords? What about other employees? Customers? Are you following NIST guidelines?

NIST, or the National Institute of Standards and Technology, offers cybersecurity guidelines that companies interested in doing business with the federal government must comply with, and that many private companies voluntarily follow. But as Damian pointed out, it can be difficult for companies with smaller budgets to do so.

> **Damian:** When I was the CISO for the DoD, in uniform, we used the NIST framework. And that was my idea going into Landry's, to use NIST. But it's not mandated, and it can take a relatively large staff and ongoing effort. So I chose an organization called CIS — the Center for Internet Security. They have a list of the top 20 security controls, broken down into tiers. Get after the top tier first, then the second and the third. If your organization has an immature security posture, that's where I would start.

> “
>
> ***Covering the basics gets harder as your organization grows;*** *the more servers, the more infrastructure you have, the more difficult it can be.*
>
> - Roy Mellinger

For high-priority components of NIST guidelines, such as password security, you can also look to security vendors that can facilitate easy alignment, without the need to augment staff.

And while a great deal of potential human error can be mitigated by focusing on security basics, employees often remain the weakest link. And surprise surprise, it turns out that annual security training alone is insufficient.

Harry: Security education was mandatory for every employee at CareFirst, and phishing email training was part of that, but unfortunately, it was a once a year exercise. We thought we were making the right investments, but we learned in the process that they weren't enough.

Roy: I think you can mitigate a lot of human error by focusing on the basics, but human error continues to cause problems. Misconfigurations, for example. There have been many, many unfortunate breaches where a system may have been secure, but they did a software upgrade and forgot to turn the security controls back on. And suddenly an attacker backs out of the URL a little bit and they've got admin access to an application.

While certain industries, such as banking and healthcare, are required to have third-party risk assessments in place, every company should have a program in place to catalog service providers that have acess to information, either directly or indirectly. That should include the right to audit.

Harry: We probably shared data with about 150 companies, all kinds of partners. You never know where the breach is going to happen. You can't just point the finger, you've got to be able to communicate and take responsibility at the same time, because it's your vendor, a vendor you chose. But at the same time, you have to place legal blame, because you don't want to be sued.

Damian: As we're negotiating initial contracts or follow-on renewals with vendors, if they're providing a security service, I try to make sure some of that risk can be transferred. As a CISO, you've got vendors coming in to pitch, and they all claim to be the best. Well, if you're the best, you need to be liable for at least the amount of money we're spending with you. Now, that doesn't always work; sometimes it's difficult to get past legal. But another approach is making sure the vendor is clear with you about how they're protecting any data you're sharing.

Roy: At Anthem and elsewhere, I've implemented a security addendum with vendors through the legal department, outlining preventative measures: we have the right to audit you, and if there's a breach, you must cooperate. I think that's table stakes to making sure that anybody you're doing business with has a sound security program. Also key is evaluating your third parties against some type of risk formula, and accessing that frequently.

Discovering the Breach

In the case of Anthem and CareFirst, hackers began with spearfishing, a sophisticated, targeted attack to deploy malware into the companies' systems.

CareFirst discovered about 70 employees with elevated privileges were targeted with a phishing email, which Harry's team detected and shut down — but not before one employee, a systems administrator, clicked through.

In the case of the Landry's breach, while the forensic investigation was never able to determine the cause, Damian believes it was likely a phishing email. And while malicious state actors were behind the healthcare companies' breaches, the criminals in the Landry's case were likely motivated by financial interest and the millions of credit card numbers the company processes every day.

Damian: About two months after I took the CISO position at Landry's, we started getting complaints from customers about credit card fraud, and we were having some weird network issues in our point of sale environment. We hired a third party; they did a forensic investigation, and were able to put together a summary and timeline of events.

> “*We knew the employee clicked through – in real time – and we thought we had shut down what occurred, but the software was so fast in downloading and traversing the network with her credentials that* ***we missed it.***
>
> - Harry Fox

For CareFirst and Anthem, the data exfiltration was brief, but the attackers had been inside for a long period of time, surveilling the system. **This dormant period appears to be a commonality among many breaches.**

Roy: The criminals had actually been inside via a number of avenues and left many of them dormant, and then when we started closing down the attack vectors, they tried reopening some of those old dormant "portals" or "windows" (which we were successful in discovering). It was clear that they had been doing their homework.

First Steps After Breach Discovery

For all three companies, pulling together teams to deal with the immediate aftermath of the breach was critical. That meant gathering internal experts to focus on the technical issues – cleaning up systems, activating disaster recovery plans, blacklisting certain web addresses, accelerating network segmentation, and reviewing all policies and procedures – as well as business-side teams devoted to legal, policy, and communications issues.

“

Being able to respond quickly, having a prepared plan, and knowing what your communication tools are going to be – **that's very much key.**

- Roy Mellinger

Roy: Part of what was key for Anthem (and what I recommend to other companies) is to have a formal breach response program in place. It’s not enough to have a data recovery or disaster recovery program. How you respond is even more scrutinized if you’re in a highly regulated industry like banking or healthcare.

Damian: Landry’s is a big PCI shop, so we had reporting requirements around that. We also hired a third-party legal team that specializes in IT security and breaches. They worked with our legal team and helped us navigate those requirements. We also beefed up our call center to accept the increased volume of callers, and we had a plan to help individual customers.

While the technical and business teams worked in parallel, they also had to work together to help translate the technical issues into messaging for each group of stakeholders, including customers, the media, and regulators.

Harry: Understanding what actually happened was complex and technical, and it wasn’t clear all at once, so we were constantly assimilating what we were learning. We worked to translate the story into plain English, and made sure our CEO understood it and was comfortable. He handled all the media, with me and the chief legal counsel sitting in the room to add color if necessary.

Roy: If you’re not controlling the communication, somebody will control it for you.

All three companies had to essentially fly the plane while they were building it – figuring out how to message what they knew, even when they didn’t yet know all the facts, to the appropriate audiences. They also found it was critical to factor in digital communication spaces like social media, not just the traditional press. In Anthem’s case, alerting elected officials early in the process earned the company goodwill when it needed it most.

Roy: We went to Washington D.C. very quickly, before the media story broke, to make sure that members of Congress were aware of what was taking place with different states’ attorney general’s offices and regulatory bodies. We let them know, ‘This is what took place, we’re going to be making a press statement, we wanted you to hear about it first.’ And I think that garnered us a lot of goodwill. The FBI and others would call that the new gold standard of how a breach should be handled. We were very transparent upfront.

Preparing for Litigation

After the immediate crises of a breach come the longer-term challenges, which can include regulatory investigations, oversight and litigation – all disruptive to the business. A great deal of time and money must be spent to deal with them, so we wanted to understand what CISOs can do to support these efforts.

Roy: You need to have a strong program, and have it documented. It's okay to have risk as long as it's identified, management knows about it, and you're working towards mitigating that risk. It's got to include internal auditing, external auditing, and the security department all working in combination – that's the three-legged stool for risk management.

It also helps to get certified by ISO or HITRUST. That's external authoritative validation, by others and not just yourself, that you are doing the right thing. It's very hard to argue in a court of law that you didn't do the right things if you're assessing your programs, testing them, and documenting them.

> “
>
> *Certain types of data are sold, like credit cards, which have a shelf life,* ***so they have to be sold quickly.***
>
> - Damian Taylor

Seeking the Missing Data

In most cases, breached data will eventually end up on the dark web, often after criminals have carefully plucked out the highest value information, which they'll use to further infiltrate certain individuals' accounts, seeking access to bank accounts or corporate trade secrets. Damian found some of the data Landry's lost on the dark web, but Harry's team at CareFirst did not.

Damian: It was me searching on the dark web; there are these popular forums where certain types of data are sold, like credit cards, which have a shelf life, so they have to be sold quickly. There are also third party organizations in the financial sector, they monitor those channels, so they also saw the information being sold on the dark web.

Harry: We were searching, really for a couple years, for specific dumps of this data. We had companies we used with arms into the dark web searching for our data, and that was true for all three of the big breaches that happened, to Anthem and Primera and CareFirst. As you know, it appears the Chinese were gathering data on U.S. citizens through these major breaches, and healthcare companies were specifically targeted.

“

Never waste a crisis.

- Harry Fox

It’s a frightening scenario. The U.S. Justice Department has indicted four Chinese hackers over these and several other large breaches, including the U.S. Office of Personnel Management, Equifax and Marriott. Combined, the alleged hackers were able to amass hundreds of millions of pieces of data on Americans. According to Wired, “By combining personnel data with travel records, health records, and credit information, Chinese intelligence has amassed in just five years a database more detailed than any nation has ever possessed about one of its adversaries.”

Long-Term Post-Breach Investment

“Never waste a crisis.” That was the overarching message we heard from each of the executives as breach response moved from the immediate to the long-term. Each company made strategic shifts as a result of the breach, including new investments, budget allocation, and program prioritization.

Damian: As a security leader, your ability to obtain additional resources becomes a lot easier right after a breach. For me, I had items on my strategic plan to address risk in the environment, and I was able to get the funding to purchase those, such as implementing a more intelligent email gateway system. We put in place two-factor authentication and updated firewalls and our secure web gateway – we were using an old one that wasn’t configured properly.

Roy: Knowing the tactics used by adversaries, there are things I am more adamant about, such as two-factor authentication and privileged account management. These are key defensive measures – table stakes, no longer ‘nice to haves.’ Another thing I’m adamant about prioritizing: a solid cyber security operations center, so you’re able to read threat signals, whether it’s an in-house team or outsourced.

It’s critical to find out quickly when a breach happens and somebody’s in your four walls. I liken it to putting speed bumps in a parking lot. The more speed bumps you have, the slower traffic is going to move, giving you more opportunity to find an anomaly and have your teams explore further.

CareFirst accelerated its existing security plans “dramatically,” said Harry, including two-factor authentication, network segmentation, a jump server program, and new email scanning software. The company also looked at more cloud-based solutions, which can be a boon especially for smaller or newer companies that don’t have the resources to build a security organization from the ground up.

Harry: One of the shifts we made in that time was to move to cloud-based vendors, to buy these things as a service. That offered faster time-to-market, and we could pull them out quickly if we didn’t like them. Some of these tools that help protect you, you don’t really know how good they are until they’re in your environment, baked into your operations.

“

It’s easy to think, ‘We’re too small to get picked on.’

- Harry Fox

But the cloud is not a panacea. Companies hoping to “lift and shift” infrastructure and applications into the cloud are learning that it’s not that easy – many apps need to be redesigned to function securely in the cloud. And there have been cloud breaches.

Roy: A lot of people thought that wasn’t going to happen, but just like any infrastructure, any technology implementation, there might be problems. How has it been installed, how mature is it, and how are you protecting it? And more importantly, if you can’t protect it, how are you monitoring what’s happening?

The Question of ROI

While looser purse strings for security investments may be one immediate result of a beach, making sure that commitment remains even as the pain of the breach recedes is critical. We asked each executive how security teams can show a return on investment for new solutions or vendors. Damian and Harry suggested ROI is the wrong way to make your case.

Harry: Don’t use ROI. You can’t do it. Reframe away from ROI, because you’ll never win there. You need to think of it as a cost of doing business. It’s a cost, but it’s going to protect you and save you from losing millions later or customer confidence or your reputation – what’s the cost of that?

But that doesn’t mean you don’t still need to show the value of your security program. You should be able to share your statistics and show how you’re making progress.

Roy: It’s okay to have gaps. You’ll never get it right 100 percent of the time, but how are you measuring to ensure that you’re raising the bar over time? To me that’s part of that strategy of communicating ROI for security investments. More than that, it’s about teaching people along the way. For instance, sharing your sample phishing messages and how the company performed, i.e. here’s the one that had the highest rate of clicks. That can really drive home the point – especially when a board member or senior executive would admit to clicking it.

Roy also recommends working with your company’s marketing team to turn your expensive security program into marketing material, goodwill and positive PR by demonstrating publicly how your company is protecting users’ privacy and identities.

Lessons Learned

No company wants to go through a breach. But the reality is, we're seeing attacks just continue to rise. As we've said ad infinitum, it's not a matter of if, just when – and any organization can be targeted.

Harry: Just remember, they didn't hire you for the good times, they hired you for the tough times. This is a time to lead, and a time to lean on all the experts within you company. You survive by leading the best you can.

Deal with the fundamentals now.

Roy: Too often, I find security solutions are deployed as a check-the-box exercise. We do it because the regulators say we need to, internal audit says we need to. But is it fully implemented? Or are we simply saying, yes, we've got DLP installed. Great! Move on to the next question.

Humans are often the weak link.

Annual training just isn't enough. CareFirst's security teams began sending out brief weekly emails, and using humorous cartoons to keep employees engaged. But recognize the limitations of education.

Harry: Take as much off your employees' plates as you can, as they'll never be as good as your security team. Try to keep the bad stuff from getting to them in the first place.

Damian: Even touching 100 percent of employees, they're still going to mess stuff up. Focus your training on the highest-risk groups.

Consider outsourcing.

Harry: Many companies don't have the resources to do what it takes – but it's possible to get protective, wraparound services at the right price. No need to build from the ground up.

100+ B
Recovered Breach Assets

22+ B
Total Passwords

26+ B
Email Addresses

50+
Breach Sources Collected Per Week

> **Damian:** If you're already looking at modernizing your IT, see what you can shift to cloud vendors. They all have strong security teams in place, far better than what you or I could provide on premises.

Have a formal breach response program in place.

> **Roy:** It's not enough to have a data recovery or disaster recovery program.
>
> **Harry:** Document everything as you go through breach recovery, so it can become replicable.

Communication is critical.

And every stakeholder will need a slightly different message. Understand you will need to begin communicating before you have all the answers. Keep regulators in the loop. Don't forget about social media. Make sure your leadership team is well educated on your message so they can share it with their teams, and with customers.

The overarching message from Roy, Harry, and Damian is this: being able to respond quickly, having a prepared plan, and knowing what your communication tools are going to be will be key to surviving a breach.

About SpyCloud

Current, Relevant, Truly Actionable Data

Think of SpyCloud as an early warning system: when your employees' or consumers' credentials have been compromised in a third-party data breach, SpyCloud flags those accounts and automates the remediation of the exposed passwords. It saves you time and reduces your exposure window substantially.

Backed by the world's most comprehensive and actionable collection of breach data and PII, our solutions let you trust that the users logging into your systems aren't criminals using stolen information.

Check your breach exposure at spycloud.com.

SpyCloud

Hungry for more?
Check out our Resource Library for guides, on-demand webinars, and case studies.