WHITE PAPER

Recovering from the Year of the Data Breach: Making 2015 Better Than 2014

Last year was arguably the worst ever for data security, and this year isn't looking great, either. Here's what happened last year and how we can improve security moving forward.

By Chris Webber

Centrify®

TABLE OF CONTENTS

Centrify®

No year in the history of the Internet was as turbulent as 2014.

There was a time when hackers broke into networks mostly for kicks, just to prove that they could do it or maybe to make some sort of statement. It was a game of bragging and humiliation, an attempt to show the world that if they really wanted to, people with excellent skills and bad intentions could really cause trouble for the rest of us. Let this be a warning, they said. And mostly, we didn't listen.

The words of the network prophets started to ring true, though, when less altruistic hacking experts figured out how to make money and cause havoc by cracking virtual safes. Big data breaches caused headaches for IT staffs. Then, they started rattling corporate executives and hitting the bottom line. Then, they caused problems for consumers. Eventually, they made news outside the tech world, and ultimately, they played a role in geopolitics and national security.

No year in the history of the Internet was as turbulent as 2014, which witnessed security breaches that brought down retail giants, caused panic in corporate boardrooms and government offices alike, and even did the seemingly impossible—delayed, and radically changed, the release of a major motion picture. It was one thing for hackers to get our credit card numbers, but to mess with our movies? Well, that was just too much. The world sat up and took notice.

It was, of course, almost too late, but not quite. While 2015 began inauspiciously in data-security circles, organizations of all kinds do have an opportunity to make data safer this year than it was last year. It's going to require some rethinking of strategies and ditching of bad, old habits—but it needs to happen now.

2014: The Year of the Breach, but Why?

The old adage in business states that it's not what you know, it's who you know. For thieving hackers, though, it's still not what you know; it's who you can become. Hacking isn't about storming the castle anymore. It's about sneaking into the castle, pretending to be a guard, and then ransacking the place. Identity is the name of the game. Log in from the outside but with the credentials of someone within an organization, and the door to the vault is wide open.

They all seemed to happen fairly quickly, these breaches, as if somebody suddenly figured out how to pull them off and everybody else jumped on the bandwagon. And that was kind of what happened. Corporations and other organizations spent lots of time and money bulking up perimeter defenses aimed at keeping evil-doers from breaking in from the outside. Then somebody on the wrong side of the law discovered that stealing users' identities is the easiest way to break into networks, and most IT staffs weren't prepared to deal with threats from the inside. In fact, in many cases, they didn't even know it was happening.

The attacks weren't even all that sophisticated. Steal a password, find an unprotected server or a server with a weak password, and everything is there for the taking—money, mainly, but also corporate secrets and all sorts of other sensitive information. Reused passwords and weak passwords were no match for thieves who wormed their way into networks. Data security in many organizations was like an M&M, tough on the outside but very soft on the inside. With no need to even crack the shell, hackers could go right to work stealing poorly protected data. This was the anatomy of pretty much every large security breach in 2014, from the famous ones to the ones that flew under the radar but nevertheless did lots of damage.

Reused passwords and weak passwords were no match for thieves who wormed their way into networks.

But wait … Weren't we supposed to be getting better at preventing this stuff? It's not as though companies and even governments haven't spent tons of money on security in recent years. It's a massive industry. What happened? They focused almost all of their efforts on the shell and not enough on the soft middle. The bank vault was made of steel, but the door to it had only a simple combination lock. It doesn't even take a super-sophisticated hacker to steal an identity and get started wreaking havoc.

Time to Make Some Changes

In 2014, criminals managed to steal millions of passwords from weakly protected networks. The same has already started in 2015. What can IT professionals do to stem the tide of breaches? First, they—and everybody else in a given organization—can ditch some bad habits. If we're going to make 2015 a safer year than 2014, we need:

Access to files and applications needs to be protected not just by a strong password but also by security tokens and biometric verification.

- **Stronger passwords.** Yes, it's that simple. We all have hundreds of passwords to manage, or so it seems, and that's just for our banking, social-media and gaming applications. Many people fall into the habit of using weak passwords, and using them over and over again. Reuse of passwords weakens their effectiveness, as does using the word "password" as a password. The password problem gets exponentially worse when IT departments have to deal with thousands of passwords, or more, and fall into the trap of password laziness. Stronger, longer, more sophisticated, unique passwords are where better data security starts, both in average users' cubicles and in data centers. IT must enforce usage of stronger passwords whether users like it or not. And famously labeling a folder full of passwords with "Passwords" probably isn't a great idea, either.

- **Multifactor Authentication.** It can't just be all about the password. Access to files and applications needs to be protected not just by a strong password but also by security tokens and biometric verification. This makes the process of simply stealing a password and accessing critical data next to impossible, or at least prohibitively difficult. It's also going to require some investment from IT and financial executives and some patience from users, but it's worth it.

- **Privilege Management.** Not everybody gets to see everything, and throwing passwords or other identifiers around to just anybody is not cool. This might sound simple, but a lot of organizations fail miserably on this front. It takes time for business and IT managers alike to decide who should get which level of access, and it's not always a smooth or easy process. But privilege is really what data thieves are after, and, as a result, organizations must make privilege management a priority. These are the keys to the castle.

Of course, the ultimate goal of network security is to ditch the password altogether and use some other form of identification, such as SAML, Ouath or Oath. That's coming. In the meantime, it's critical for IT to shore up the security measures it has in place.

It's not about the Perimeter

Breaking old habits will help make networks safer, but it's not a panacea. Organizations still need to completely rethink their approaches to data security. That means focusing much less on perimeter security and concentrating much more on internal defenses, such as access management.

The perimeter should already be secure in most organizations given how much they've invested in the defense of it, but that really doesn't matter much anymore. What matters now is what users who have credentials can access and how they can access it. Hackers assume the identity of these users to enter a network and do real damage. That's why password strength is important, but so is the idea of automatic provisioning. Let's remember, too, that rogue employees can very much be the cause of data-breach problems. Some internal threats really do come from the inside—maybe most of them. Trust nobody and keep access to applications on a tight leash.

What matters now is what users who have credentials can access and how they can access it.

Of course, it's easy to talk about access management, but implementing it is something else altogether. There is no shortage of solutions available to control access, privilege management and other areas of user authentication and control. Just getting started can be confusing to the point of frustration. It doesn't have to be, though.

The key in setting up any solid data defense is to take a simple but thorough look at the organization. Ask and answer these questions:

- What are the organization's critical resources? What's deeply important, and what's less important? Focus on protecting the crown jewels of data first before getting to lesser assets.

- Is the data-security setup protecting them? How vulnerable is the organization to data theft? Think critically about the new ways criminals are stealing data—by impersonating users, or sometimes by just being users—when answering this question. It's not just about keeping the outside safe anymore. Could impostors pose as guards in the castle and steal the gold?

- Is the right password-management system in place? We've seen that passwords are important. Managing them is even more important. Users will revert to type and be lazy with passwords. IT can't let them. Security teams need strong passwords and need to know who has which ones. That makes a potential breach much easier to pinpoint.

Start work internally to solve these issues, and then move to the perimeter. This is a complete about-face compared to what IT has largely done over the last couple of decades, but it's the kind of rethinking about security that is necessary today.

Focusing more on internal security and less on the perimeter is critical.

A New Era for Data Security

Organizations of all sorts need to put 2014, the worst year in the history of data security, behind them. To do that, though, they need to break some bad habits and seriously rethink and reconfigure their security strategies. Focusing more on internal security and less on the perimeter is critical, as the nature of attacks has changed. Nobody wants to suffer the next big breach. Organizations that take the time to rethink security are the ones that will keep themselves out of the headlines. ■

Chris Webber is chief security strategist at Centrify. Chris is a security wonk, a cloud evangelist, a product guy, and a recovering IT professional. Having spent time at both Silicon Valley startups and global powerhouses, he developed his particular slant on cloud and mobile security at companies like Zscaler, Blue Coat Systems, Good Technology, and Pertino.

Centrify®