Harvard Business Review

REPRINT H02834
PUBLISHED ON HBR.ORG
JULY 27, 2015

ARTICLE
SECURITY & PRIVACY

Why Cybersecurity Is So Difficult to Get Right

by JM Olejarz

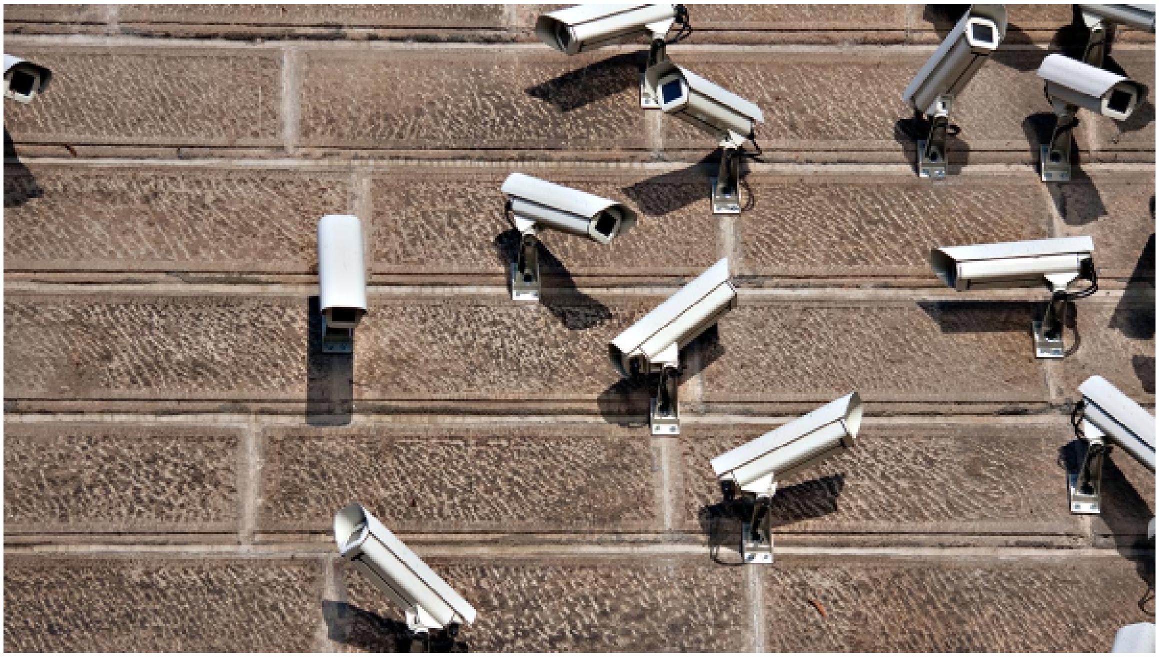
Harvard Business Review

SECURITY & PRIVACY

Why Cybersecurity Is So Difficult to Get Right

by JM Olejarz

JULY 27, 2015



It seems like hardly a week goes by without news of a data breach at yet another company. And it seems more and more common for breaches to break records in the amount of information stolen. If you're a company trying to secure your data, where do you start? What should you think about? To answer these questions, I talked to Marc van Zadelhoff, VP of IBM Security, about the current state of cybersecurity and the Ponemon Institute's 2015 study of cybersecurity around the world, which IBM sponsored.

HBR: Did the study find any new trends in cybersecurity?

Marc van Zadelhoff: We have a large business dedicated to security and so we see even beyond the study, across thousands and thousands of customers that we monitor daily. One of the major things that we've seen over the last few years is how breaches are increasingly done by ever-more-sophisticated organized criminals. Forty-five percent of breaches occur because of criminals breaking in, so one of the reasons why the cost of breaches goes up is because we're seeing more being caused by crime, as opposed to other factors like inadvertent mistakes.

It's one thing to have a breach because an employee loses a laptop, but more and more of it is organized criminals who are very persistent in their approach. For example, when a criminal is involved, the cost for a breach is typically $170.00 per capita per breach, versus if it's a system glitch or a human error it's more like $140.00 a breach. It becomes more expensive because they steal more, they're more persistent, they're stealthy, they stick around, they're harder to detect and harder to get rid of. It's like a more difficult virus in your body. The best advanced attacks on our organization are just harder to inoculate against, and harder to get out of the system.

I'm surprised that the percentage of breaches caused by attackers isn't higher. If you read the headlines in the papers, it seems like those are the ones you tend to hear about the most.

If you're getting breached, there's an incentive to talk about it as being an attack as opposed to a mistake. So I think that's why the ones that do get covered a lot in the press are the ones where companies come forward and say, "Somebody spent a lot of time and did a professional job on us." I think people get a little less vocal when it's truly a mistake.

What about the breaches caused by mistakes, the ones you don't hear about as much?

I think that not enough attention is being drawn to the careless exposure of data by internal mistakes—which happens quite often, even when there are no malicious actors prompting it. Aside from the most obvious slip-ups, such as leaving passwords in plain view or failing to report a lost or stolen corporate device, many people today are uploading personal and corporate information into third-party, collaborative platforms without thinking twice about how secure this action might be. While these tools are giving us a wealth of opportunity when it comes to working more efficiently and collaboratively, we have to remember to always be cautious in regards to how we're using, sharing, and collecting data.

What are cybercriminals usually after? What should companies be protecting?

In general, organized criminals are trying to steal things of high value, and one of the most valuable industries, in terms of cost, is health care. So what you see is that criminals are going after health records because on the black market they can probably sell a health record of a person for about $50. If they only steal credit card data or a social security number, they might be able to sell that on the black market for $1. Or they may steal a health care record not to sell it, but to leverage that information to do a more sophisticated attack on you. They might impersonate a bank, saying, "Hey, I know you're about to go and get an operation, don't forget to transfer some money by clicking here," or whatever. And then you think, "Well, they know I'm having an operation tomorrow, so they must be a legitimate bank." So the initial crime results in more valuable data leaving the building.

If health care records are worth so much, why do hackers go after anything else?

While health records themselves are worth a lot on the Dark Web, there are other types of high-value data that can be pieced together to be used in sophisticated attacks. These types of information can be used to conduct malicious activities such as social engineering, creating dossiers on high-profile figures (with the end game to disrupt their lives in a malicious way), stealing identities, damaging a corporate brand, and more. Businesses of all types and sizes must seek to understand what types of information they have that would be of most value to hackers, as well as what would be most damaging to their company, employees, and customers if a breach occurs. By taking this first step of defining what is most important and where it resides, organizations can then personalize their security programs to adequately protect their unique "crown jewels."

The study found that the factor with the highest impact on the per capita cost of a breach is employee training. Is that IT people's training or the standard security training that everybody gets?

Both. You've probably had security training at work, maybe even been tested at the end of that training in terms of remembering things. But you can test people more throughout the year, and you can try to "trick" them. For example, we work with customers to do kind of a phishing attack on employees. It's a way to see what employees click on in an email. We might send you an email saying, "Hey, I see you're heading to California next week, click here to confirm your travel." And we would have figured that out because you posted on Facebook that you're headed to California. Well, if you click on that, since it's your company doing it, a prompt will come up and say: "This actually a phishing attack, you should always look at the header and who's sending it before clicking on anything." So it's a way of testing without it actually being an attempted hack.

If you have employees aware and a little bit paranoid, it can make a big difference. And often the more senior employees at an organization are the ones that are just less socially aware, in terms of Facebook and LinkedIn and all these things. They can be quite susceptible to still clicking on things, or assuming that if someone sends you an email and it has a couple of pieces of data that are accurate, that it must be legitimate.

Recent attacks on OPM and a London hedge fund show two different ways that cybersecurity is so difficult right now: First, even the U.S. government isn't safe from attack, and second, the hedge fund's CFO was able to be fooled into giving away information over the phone. If you're a company following those stories, what should you take away from them?

The first takeaway from those breaches would be that today's cybercrime gangs are brazen and operate with organization and sophistication like that of a well-funded company.

Employees can be seen as the Achilles' heel of cybersecurity; mistakes by those with access to a company's systems are the catalyst for 95% of all incidents. It can be as simple as accidentally clicking on a malicious link or failing to question the authenticity of a phone call or banking website. Even organizations with the most robust, forward-thinking security strategies aren't immune to one lapse in employee judgment.

It's critical that in addition to a strong technical security defense, companies should continuously educate employees on the dangers of security attacks, ensuring that they know what to look for and how not to fall prey to social engineering. They should continuously review and keep tabs on which employees have access to sensitive data, and ensure access is removed instantly once an individual disassociates with the organization, or changes roles to one that doesn't require the same level of access.

As you've studied security around the world, what are the best practices that companies should be following?

Best practices are, first, having very good analytics and intelligence in place. You need to have probes available to get you information either as the data breach is occurring or afterwards, to be able to understand the damage. Next, having an incident response team that is trained and ready for the scenario of a breach. Like your kids at school practicing fire drills, you practice getting breached so if a breach occurs, you know, OK, she's going to be in charge, he's going to be the face to the press, and Larry and Sue are going to call the FBI. Companies that had a response team had an average $12 or $13 less expensive cost of a breach per capita than companies that didn't.

Third is the use of encryption. If you have encryption layered on your data, maybe they get a user name, the password, maybe they get a social security number, but the health care record is actually encrypted. So they stole $1 worth of data, but they didn't get the $50 worth of data.

Fourth is employee training. Fifth, all organizations have a business continuity management team. If there's a tornado or a hurricane, they're able to help companies stay up and running. Well, having them involved when there's a breach is a best practice. And then finally, Board-level involvement. For example, say you got breached and went to the marketing department and said: "We need to shut down a particular database with customer data that's often accessed." They might look at you and say, well, why? But if you've taken the time beforehand to prepare and say, during a breach scenario, here are the things that we're going to do, that can make a big difference,

And if you're a company planning your security efforts, what should your goal be? Can you actually defend against getting hacked?

The reality today is that no matter how careful we are, no matter how well we design our strategies or how thoroughly we educate and engage employees, we're never 100% safe against a cyber-attack. Our best defense is to revamp how we've been approaching security, and to move from constantly bombarded, isolated defensive positions to a united, intelligence-driven collaborative front against cybercrime.

We need to begin thinking like the hackers that are so successfully penetrating companies. Hackers use the Dark Web underground network to share data, expertise, and resources. Using collaboration, they've formed complex and highly efficient cybercrime rings, from which 80% of malicious campaigns start. The private sector is still largely working in silos, with no visibility as to what attacks are on the horizon until they hit.

To truly fight back as best as we can, we need to collaborate on the same level as hackers, sharing information across industries and organizations to see attacks in real time. Just like a disease epidemic, if we're able to put the right infrastructure, warnings, and precautions in place before a malicious attack comes to us, chances are that we'll be much better equipped to spot it and shut it down if it does get into our systems.

JM Olejarz is an assistant editor at *Harvard Business Review*.