What to Expect When You’re Expecting a Data Breach

END OF YEAR REPORT FROM ZERONORTH
Chapter 1: The New Landscape

From security threats to compliance regulations to the unrelenting pace of business, staying conscious of cybersecurity risks in 2020 is shaping up to be a full-time job. Around this time of year, experts love to offer up their predictions about what’s on the digital horizon and how we can best prepare ourselves for the inevitable future. Whether or not these apocalyptic cybersecurity situations come to fruition remains to be seen, but one thing’s for sure—it will be a year to watch.

As the U.S. presidential election, and all the security implications it carries, takes center stage, many of our shared concerns around risk and vulnerability will come into sharper focus. Which big corporation will fall victim to a breach? Will users ever gain control over their personal data? Who will win the war on cyber terrorism? The hot button topics are endless, making 2020 the year when several security trends are likely to converge to create an entirely new landscape of cyber threat—and fortunately for us, cyber solution.
Let’s start with the statistics. More than 9,100 data breaches, containing more than 10.4 billion exposed records have been made public since 2005, and they are costly. Research from Kaspersky illustrates how the cost of an average breach is up from $1.23 million in 2017 to $1.41 million in 2018—and according to Cybersecurity Ventures, cybercrime will cost the global economy $6 trillion annually by 2021, up from $3 trillion in 2015. Exacerbating these problems is the continued cybersecurity skills shortage on top of an increasingly interconnected world. While these numbers are alarming, they are also just a reminder of what we already know—the speed and sophistication of digital threats are growing, not to mention they are slated to create increasingly significant financial headaches.

And as our digital landscape continues to expand, so too will the Internet of Things (IoT), now poised to introduce billions of new devices into the environment, all of which will become potential targets for attack. According to a recent Newsweek article, 2018 saw the global installment of more than 23 billion IoT devices, a number that is expected to hit 75 billion by 2025. Unlike the “internet of computers,” which was created largely by technicians with IT experience, many of these IoT devices are being manufactured by an industry more focused on revenue than risk, with limited expertise in what it takes to build airtight systems. In truth, the majority of IoT vendors don’t recognize the importance of creating bullet-proof products, and as a result, the possibilities for mischief are endless.

With such realities on the horizon, it doesn’t take an expert to predict there are going to be some serious security issues in the coming year. It’s not a matter of if, but when. And so, like any good practitioner with a seasoned sense of reality, the question of what’s ahead really revolves around how to control the inevitable. What we can’t do is predict the future, but what we can do is prepare ourselves for a wild ride by stuffing our back pockets with meaningful strategies for success. And a big part of this vigilance comes from just knowing what to expect when you’re expecting the unexpected.
Chapter 2: Asking the Right Questions

Am I secure? Am I compliant? Understanding today’s security landscape, and your place in it, involves asking tough questions about the state of your digital preparedness. While we would all love the ability to visualize our digital strength in one glance, just answering these yes or no questions will not achieve that goal—because the unfortunate reality is, many organizations still view risk in silos, which means they can’t really visualize their own attack surface in the first place.

The challenge then becomes to ask yourself different questions, even harder ones, that push you towards identifying and understanding all the vulnerabilities you face, across both applications and infrastructure. If you need a comprehensive answer to security in the coming year, which you most certainly do, you will need to dig deeper into what it takes to meet the new challenges of 2020:

**Am I set up for growth?**

If you’re looking to expand your business, software is the answer. It will help
you push into new areas of industry and drive your enterprise forward. Sounds simple enough, but there’s a catch. As you rush to roll out exciting new products and services, you will also need to increase the velocity by which you bring software to market. This type of rapid growth means rapid application development cycles—rapid everything. And security, as we know, doesn’t always translate in this type of “everything now” environment. So, regardless of how prepared you are to push out that new product in 2020, the integrity of the software behind it must garner the same level of attention.

In 2020, we expect to see more companies moving away from manually writing code to using software tools to create applications and websites. While this is great news for those looking to use software as a competitive differentiator, it also means vulnerabilities can be exploited on a much wider scale. Planning ahead is key to the success of future growth, especially when it comes to application security. And to ensure that growth is successful and sustainable, you need a strategy for how to scale and adapt using both new and old tools—without compromising any of your security and compliance-related responsibilities.

Should I Sacrifice Security for Speed?
As the new year kicks in, everyone will be looking to move fast, especially because increased speed often becomes the key differentiator in success. This is easy to say, but hard to execute. Software, and the infrastructure it runs on, is a critical asset, which means continuous deployment is essential. But as companies rush to ship products quickly and meet their product obligations, this velocity and frequency often leads to inept or even negligent security within the software releases themselves. And suddenly moving quickly isn’t possible without sacrificing security, making the need to simply “move fast” an unsustainable and ineffective approach. Because no matter how exciting that new product promises to be, to both customers and your bottom line, there’s no room in 2020 for bad security hygiene and negligent practices.
Does Compliance Equal Security?

Unfortunately, compliance questions in 2020 will be about as easy to answer as security ones. Right now, companies deploy a wide range of tools to monitor application security (AppSec), while different vulnerability management and penetration tools identify threats across infrastructure. The result is a lot of data, but not necessarily the kind needed to answer hard questions.

Despite the copious nature of these findings, there is still no complete and actionable view of application and infrastructure risk. The new year will force us to replace more information with better information, as we look for ways to address the exploitable findings affecting our security posture. By removing the overwhelming mountain of triage and busywork associated with ineffective security tools, we give ourselves a new level of clarity into what really matters. And a result, the organizations most at risk will be those who rely heavily on mere compliance and fail to arm themselves with solid plans for incident response.

Do I Need More Technology?

In today’s era of fast everything, a go-to solution for many businesses has involved simply throwing in more security tools to see what works. Rather than boosting the efficacy of what exists, organizations just add more and more solutions, hoping security will eventually “take.” In fact, new research from ReliaQuest found that 71% of security decision makers are adding security technologies faster than they are adding the capacity to productively use them. This type of reactive behavior stems from weariness rather than wisdom, and does not address the real issue. And it certainly does not tee up success in the new year.

The modern problem we face is not a lack of technology—but rather, the inability to utilize our existing technology to achieve quality results. Tackling security takes a lot of manpower. It’s time-consuming, expensive and demands the full attention of skilled professionals. This means organizations
with highly-fragmented and limited views into specific components of their stack will inevitably face more risk. Yes, they have a number of tools at their disposal, all of which possess their own unique functions and process, but they do not have the resources to manage such an unwieldy process of discovery and remediation. They are not asking the right questions. Yes, different scanning tools address various layers of the software development lifecycle (SDLC), with disparate methods for rating vulnerabilities, but this overlap leads to inefficient reporting and action, as resource-strapped developers struggle to make sense of their findings.

In this way, 2020 promises to deliver a lot of frustration, especially for businesses looking to correlate and simplify the remediation process. Trying to normalize results from all these different tools is currently a challenge that will only grow as new applications are added. As your ecosystem, not to mention your responsibility, also expands with move-to-cloud initiatives and microservices, it is critical to understand how already-overtaxed security experts will fail to keep up in the new year.

As a result, some industry professionals suggest a combination of microservices and development monitoring will emerge in 2020, as more people recognize how their siloed logging data offers them a narrow view of security. And a result, there will be a lot of folks looking to switch up their security processes, ditching conventional methods of high cost and no scalability to embrace something more holistic and sustainable.
Chapter 3: Finding Tricky Answers

Now that you recognize how tricky finding answers in the new year will be, it’s time to develop a plan. But how? Where? You want to manage for success, but you can’t manage what you can’t measure. The good news is, you’re not alone. Even the most digitally-advanced companies often don’t have a well-defined approach to guarantee software security. In truth, building security into the software development process requires developers, IT operations and security teams to work collaboratively to ensure security is integrated in a way that doesn’t impede the fast delivery of new software—or its functionality. To this end, vulnerabilities at all stages of the SDLC must be identified before deployment, and you must be able to confidently answer these questions:

1. When new applications and capabilities are rolled out, how is security addressed?
2. Is cyber resilience considered throughout the development process?
3. Is there a consistent methodology for validating the security of new applications?
Yes and no questions won’t cut it in 2020. You will need to know how and where security is addressed during all stages of the SDLC, with the type of evidence-based conclusions needed for compliance and overall reporting. Lack of clarity in any of these areas will only lead to ineffective processes and unsecure systems. Next year, we’ll see more security initiatives focus on integrating static scanning technologies into software-defined containers and build and deployment pipelines.

2020 will be about using your time wisely. You will need to prioritize security through a firm understanding of the problems that impact your organization the most. Every business is different. Many scanning tools used by IT, security and developer teams report issues that have little to no impact on security. Although there are valid reasons for this, you will need to decide which issues matter most to your enterprise—and equally as important, if your tool reports match those risk sensitivities. It doesn’t make sense to spend time reading results that are unlikely to affect your business.

Lastly, you have to create and codify a methodology to facilitate the vulnerability management process. And this involves more questions. How will the bugs and flaws be fixed? How will you report on these remediations? What teams need to be involved in these efforts? Again, this process should be based on your organization’s specific risk threshold—and custom-built to support those objectives.
Chapter 4: Making the Right Moves

By now, it should be crystal clear that 2020 is about asking hard questions, using your time wisely, and shoring up security to address real risk—a larger effort that requires more than just new tools and methods. It will demand a shift in perspective and really, a shift in culture. In the industry, we’ve seen this change happening more and more as organizations continue to embrace DevSecOps, essentially thinking about application and infrastructure security from the start. But DevSecOps is not just about job titles or tools. It represents a significant departure from old ways and an adoption of both mechanical and holistic processes to produce a DevOps cyborg capable of squeezing out every advantage over an adversary. In 2020, we will likely see more organizations, development teams and business units embracing this concept and shifting their DevOps culture to be more collaborative and effective.

As you look at vendors next year, remember, you probably don’t need more reports or security tools. You need to extend the value of your existing ones. The year 2020 will be about orchestration and the way it eliminates the need to manually evaluate, deploy
and manage a host of different scanning and testing tools. Orchestration is what allows security teams with limited bandwidth to refocus their effort and skills on more business-critical priorities, while their companies rapidly scale the security of new applications and infrastructure to meet modern demands.

In short, 2020 will be about making security work for you, about finding real solutions that work for you. As we look ahead, it will be critical to consider risk-based vulnerability orchestration and how it empowers us to manage our tools in one single process, on one single platform. This unified approach offers a way to “try before you buy” and find the right AppSec tool to fill any scanning portfolio gaps. With this type of vulnerability orchestration, you can deploy several open source software (OSS) and vendor solutions on a trial basis, run them simultaneously on a unified platform and see which one best suits your unique environment.

The orchestration process not only allows you to pump all of your nerve data into one place, it empowers you to find the skills and techniques necessary to make sense of the evolving digital landscape. Because at the end of the day, the new year will be about honing your cyber-jutsu to ensure you are always expecting the unexpected.
ZeroNorth is the industry’s first provider of risk-based vulnerability across applications and infrastructure. By orchestrating scanning tools throughout the entire software lifecycle, ZeroNorth provides a comprehensive, continuous view of risk and reduces costs associated with managing disparate technologies. ZeroNorth empowers customers to rapidly scale application and infrastructure security while integrating seamlessly into developer environments to simplify and verify remediation. For more information, follow ZeroNorth on Twitter (@ZeroNorthSec), LinkedIn or visit www.zeronorth.io