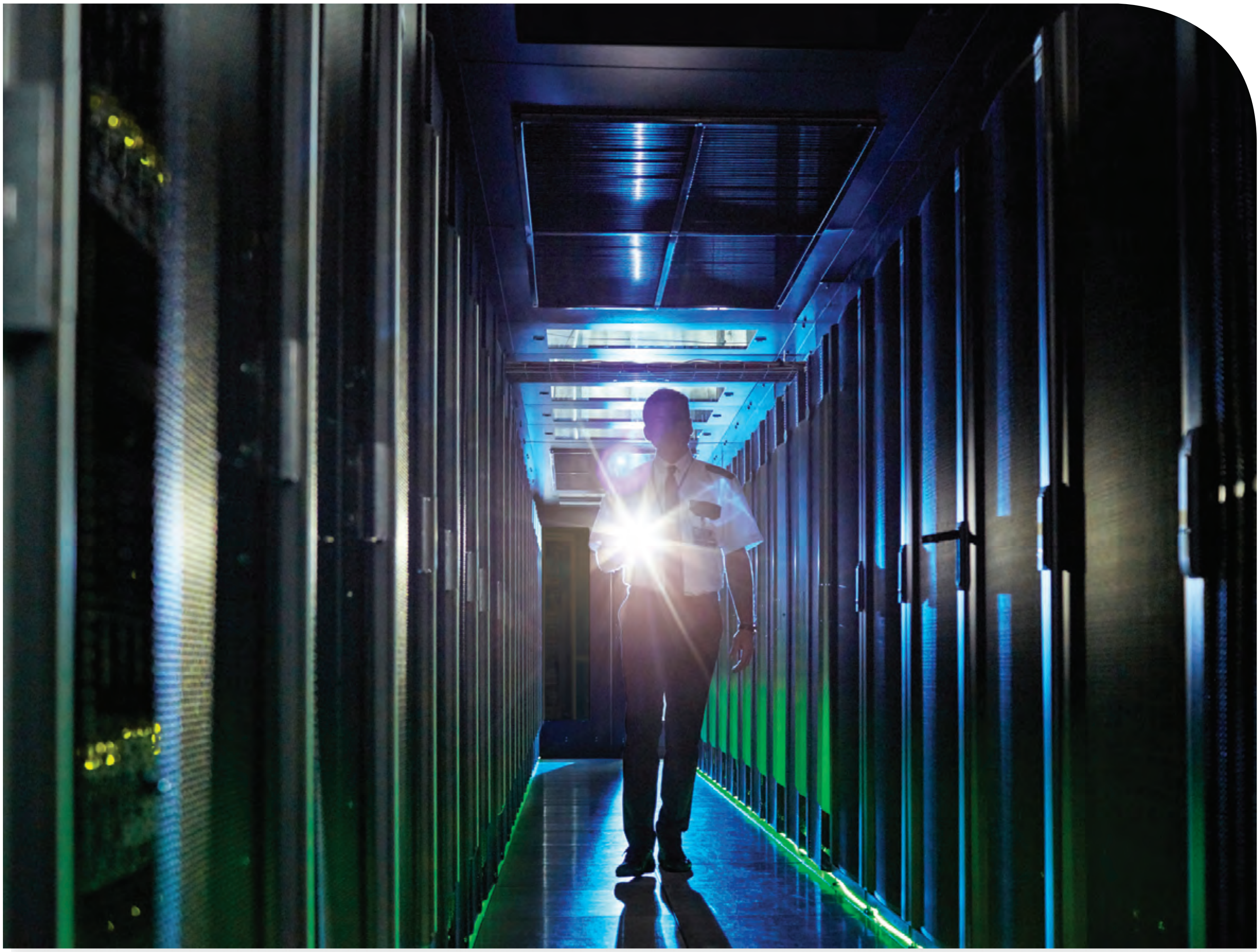

POINT OF VIEW:

Security and Compliance Mandates Can Be Draining. Here's How to Recharge.

5 Steps to protect your business — and your sanity

By Katie McCullough, Chief Information Security Officer, OneNeck IT Solutions

OneNeck®
IT SOLUTIONS
a TDS® Company

By Katie McCullough, Chief Information Security Officer, OneNeck® IT Solutions

No doubt you're aware of how frequent, damaging, and costly data breaches are. On any given day, you need only open a newspaper or scroll through your news feed to see that a new ransomware attack, phishing scheme, or other breach has affected millions or even hundreds of millions of people. Headlines focus primarily on the big names — such as Target, Yahoo, and Equifax — but small and medium-sized companies are hit every day too.

Given the daily onslaught of corporate breaches, as well as new privacy laws and regulations such as the General Data Protection Regulation (GDPR), it's easy to become numb to the risks and responsibilities in the security and compliance sphere.

How can you keep up and prevent your company from being the next to suffer a data breach or fail a compliance audit — and end up on the front page for the wrong reason? There are a number of simple yet effective steps you can take right now to regain your focus and control, even as cyber challenges continue to mount. Let's begin.

Fundamentals remain key in this era of shifting threats

By now it's a cliché to say it's "not a question of if, but when" a security or compliance issue will affect your company. Every year, attacks become more common, more pervasive, more sophisticated — and yes, more damaging.

The Cisco 2018 Annual Cybersecurity Report notes the unprecedented levels of sophistication and impact of malware, the rapid evolution of ransomware, and new vulnerabilities in unpatched and unmonitored internet of things (IoT) devices. With so many threats coming from all directions, a Ponemon Institute 2017 Research Report estimates a probability of 27.7% that organizations in its global survey will suffer a data breach within the next 24 months.

In addition to concerns about security breaches, companies are challenged by compliance and audit concerns, especially with the implementation of GDPR and the addition of new state regulations layered onto HIPAA, PCI, ISO 27001 and SOC 1 and 2. Especially for companies operating in the global market, it can be time-consuming and costly to adhere to all of the regulations and industry standards as new ones are continually added and existing requirements evolve and shift.

Even as the market shifts, you can go a long way toward shoring up your defenses simply by focusing on a few fundamentals.

One fundamental is to keep your software up to date — not only your operating systems but also every application your company relies on. Some companies think they can deploy patches on a quarterly basis or put them off indefinitely because they want to avoid downtime, but we've seen how costly such decisions can be. The enormous Equifax breach happened because the company failed to update with a known patch. Likewise, a patch for the WannaCry ransomware cryptoworm was available a month before the attack, which only spared the companies that installed the patch right away.

Another fundamental is to educate and train employees to avoid phishing schemes, instead of simply relying on technologies to detect and prevent attacks. Phishing is one of the top ways attackers exploit companies, and your end users are an attractive point of entry. Many companies have recognized this threat and are educating workers not to click suspicious emails. However, that training must be constantly reinforced and repeated, preferably with real-world exercises to reinforce the message.

And keep in mind that compliance measures are not just an operational burden — properly following GDPR, HIPAA, PCI, and all the other regulations your industry must satisfy will help you be safer. When you document your processes, train team members on your processes, and monitor your security operations through metrics and inspection to assure adherence to compliance requirements, you are laying a solid foundation for security best practices across your company.

Finally, be sure to develop an incident response plan so you will know exactly what steps to follow in the event that your data is compromised. To develop the plan, you'll want to conduct a thorough gap analysis and then identify your incident response team roles and responsibilities. By developing a solid and credible response plan, you can respond to threats quickly and still stay focused on business-forward initiatives.

5 Steps to Recharge Your Security and Compliance Efforts

Now that you've got the fundamentals down, it's time to lay out the five steps to recharge and reinvigorate your efforts, avoiding the stagnation that can lead to major breaches and fines.

1. Protect yourself in the cloud

Many companies are shifting some or all of their data to one or multiple clouds and cloud providers, which can create new vulnerabilities. It's not that moving to the cloud is dangerous — in fact, it is often the safest and most secure option for storing data — but you have to be savvy about the security measures you can control in your cloud environments, and then establish consistent processes to protect the data you house there.

Maybe because the information is often buried in 150-page operating manuals or 50-page contracts, some companies fail to do their due diligence in identifying available configuration parameters in their cloud environments. In addition to taking the time to fully understand the parameters, you should also perform regular scans of your entire environment. Regular scanning is one of the best and most underused ways to identify potential gaps and vulnerabilities in cloud environments.

2. Get an outside perspective

When it comes to implementing and maintaining rock-solid security and compliance practices, your job is never done. There is always a new technology or process that you could or should be implementing, and there are always new threats or risks emerging that you have yet to take under consideration.

The ever-evolving threat landscape is why we invite third parties to test, audit and validate our security measures at OneNeck. It is simply too easy to lose perspective and overlook valid concerns if you try to assess your own security and compliance risks. In our experience, third parties have been a wise and valuable investment. They've helped us identify gaps early and continually refine our processes.

3. Shore up your governance

As a managed service provider, OneNeck lives and breathes governance. We have workers all over the country who must respond, at any time of the day or night, to a variety of incident types in exactly the same flawless manner. To achieve that level of consistency, you must have solid governance in place.

Governance involves documentation, training and inspection. You need to be sure that every task is documented, that all your workers are fully trained, and that you have a thorough inspection process to ensure adherence, from ad hoc auditing to physical on-site team inspections. From there, you must commit to continual improvement to ensure that everyone understands the guidelines and is operating in the same way across all your locations.

4. Stay on top of compliance mandates

It is difficult to keep pace with new and changing mandates such as GDPR and the new regulations out of states such as California — which unfortunately does not give you an excuse if you fall out of compliance. Larger businesses can bring together a team of experts from their legal, human resources, financial, IT and other departments to understand the regulations, implement the right infrastructure, and design appropriate policies and procedures. But not every company has that luxury.

For small and medium businesses, new and shifting compliance mandates create a much larger challenge. As mentioned earlier, that's why so many companies are turning to third parties that have the experience and network of resources available to fully understand the requirements and determine how to ensure compliance most efficiently and cost-effectively.

5. Get the board on board

Staying on top of the latest security and compliance challenges comes at a high and ever-increasing cost — a cost that must be justified to the C-suite and the board of directors. To have a successful conversation with management, it is essential that you frame the need for security expenditures in terms they will understand. One key is to focus on business risks, not IT risks. If you can put those business risks in dollars and cents, you are far more likely to get the attention and commitment you're looking for.

Leading government contractor revitalizes its compliance efforts

OneNeck is working with a manufacturing company that was struggling to comply with NIST SP-800-171, the U.S. Defense Department (DoD) requirement that all businesses contracting and subcontracting to the DoD demonstrate that they can adequately protect Controlled Uncontrolled Information, or CUI.

To appreciate the scope of the challenge, consider that the standards establish mandates in 14 families of security requirements, including access, awareness and training, identification and authentication, and configuration. The stakes for our client were extremely high: If the company failed to comply, they would lose their DoD contract.

Fortunately, the standards in our managed services were already addressing 60% of our client's compliance requirements, including incident, change, and access management. We found that another 20% of their needs could be met by refreshing devices and performing a variety of other implementation projects. And finally, we helped them accomplish the remainder of the tasks by providing the processes and tools they needed in addition to our managed services — processes and tools that OneNeck has deep experience with.

Through a highly collaborative process, OneNeck worked with the client to put plans in place to address its NIST SP-800-171 compliance needs. Along the way, we also helped their IT department build a business case for better controlling and segmenting their cloud environment, and we put in place compliance and security elements that improved their overall data security, integrity, and confidentiality.

You can also use your own facts and figures based on event monitoring tools, which can track the attack or infiltration attempts that no doubt occur on a daily basis at your company. Showing logs of those events is an effective way to illustrate that, while your defenses may be working right now, it is entirely possible, or even probable, that within a year a costly attack will get through. You can then build a defensible case based on realistic probabilities and real-world business risks — which is far more likely to get the attention of executives and the board.

Breathe new life into your security and compliance efforts

It is easy to be overwhelmed by the security threats and data breaches that take place every day, at every size of business, in every corner of the world. Yes, the threats are increasing in number and sophistication. Yes, your business will almost certainly be attacked at some point, if it hasn't been already. How you choose to respond to the rising tide of threats and requirements — by becoming numb to them or by reinvigorating your efforts to prepare and respond — will directly affect your future success.

By returning to fundamentals and following the five steps highlighted here, you can better protect yourself in the cloud, gain an outside perspective on your security measures, shore up your governance, stay on top of compliance mandates, and earn budgetary support from the C-suite and board. In the end, that may be all you need.

Learn more

Looking for help from a security and compliance leader who practices exactly what we preach? Get details on OneNeck's Virtual CISO service.

Download the 2018 Cisco Annual Cybersecurity Report.

OneNeck®
IT SOLUTIONS
a TDS® Company

(855) ONE-NECK

WWW.ONENECK.COM