Secureworks®

GUIDE

5 Security Recommendations for CIOs Managing a Digital Transformation Program

“In the process of doing digital transformation, a CIO has to look across all the goals he or she is trying to accomplish and ask: ‘Do I have the skillsets and capacity to execute?’’

Mark Wood,
Sr. Director, Strategy and Corporate Development, Secureworks

Considering Security When Planning Digital Transformation

All businesses, with their CIOs at the helm, are undergoing digital transformation in some capacity. While security is one variable among many that needs to be considered, it is not the only one. Agility, cost reduction, and innovating new capabilities are just a few drivers for digital transformation.

Although the CIO is focused on business growth, security needs to follow along with every organization's transformation as closely as possible. Undergoing digital transformation forces all organizations to do business in an entirely new way that consequently poses new security challenges; challenges leadership may not have considered. Often, many businesses who are putting a lot of effort into digital initiatives quickly realize they lack the operations strategy, expertise, or capabilities that are needed to properly bring security into the innovation equation. It is at this juncture that evaluating third-party security partners for support becomes important. However, viewing security as part of your digital transformation principles as early as possible will make the path smoother and easier.

Historically, cost reduction was a major incentive for relying on a cyber security partner. Cost is still a factor today, but digital transformation initiatives have shifted the focus to technical skills and achieving agility. If you're going into the cloud, IoT space, or big data analytics, for example, building out those capabilities entirely in house will prove difficult.

Today, security is a far more active consideration. In fact, focus on managing operational risk and compliance has increased by 12%, while focus on improving cybersecurity has increased 23% among enterprises from 2017 to 2018 (KPMG). Regardless of whether you choose to build an in-house capability or use a security partner, the pressure is on to improve security.

34%

of enterprises' primary barrier to digital progress is data privacy and security concerns

27%

of enterprises' primary barrier to digital progress is lack of in-house skillsets and expertise – Dell

ONE

If you think you're going to need security services, explore this option early on.

Many organizations continue to operate under the assumption that it is possible to manage security internally in the digital world, but the reality is, the vast majority of even the largest businesses are simply not well-equipped to do so effectively. In fact, there is a classic pattern many security decision makers experience:

- Buy a security solution or technology
- Deploy it
- Realize cost of ownership –or— capability gap is greater than expected

A few pieces of guidance for CIOs considering a technology investment:

- Look at the total cost of operation before you buy the technology.
- Technology alone will not make you successful in security. It is not possible to buy a security solution that will make your problems go away.
- If you hire a services company to handle security in its entirety, it will be very expensive.
- In the planning stages, determine what combination of technology, intelligence, and services you need to be successful. Choose a security partner under the assumption that you need to have all three.
- Invest in upfront planning through a well-managed procurement program with business and functional requirement definitions, RFIs and RFPs, negotiations and contracts. Investing upfront will reduce pain later.

TWO

When you use a security partner, understand that you still own the risk.

So, you've decided to use a security partner to close gaps and reduce risk. This doesn't mean the risks to your business are no longer your organization's responsibility.

You can throw people, budget, technology, or some combination at a security problem. You can certainly make a significant dent in the security problem. However, it's not possible to achieve 100% coverage through a security partner. At the end of the day, there will always be necessary fixes. Furthermore, regardless of the combination of technology, services, and intelligence you use to solve security problems, those problems are still your organization's. You can enlist help, but if there's a problem, your organization must take ownership of the resolution.

It's essential to re-position your thinking to an integration with your security partner, where together you are working on managing the cyber risks to the business and reporting upwards to management and executives as a team. Making your security partner your strategic advisor usually leads to more value out of the relationship.

“If you invest more in clarity upfront, you’ll avoid a lot of wasted time and missed opportunities. Find out exactly where your gaps are and what you need to focus on.”

Hasi Hosn,
Director, Cyber Security Solutions EMEA, Secureworks

THREE

Decide upfront how to split SecOps responsibilities between your in-house team and your security partner.

Let's look at a brief case example of a hypothetical organization who leverages a security partner. The customer uses an MSSP for perimeter, network and endpoint security monitoring. They have an in-house team performing incident analysis and triage and another team handling internal user behavior monitoring and analytics. They leverage an incident response retainer from a security partner for forensics and technical incident investigations. These functions combined make up their security operations. This is a hybrid security operations delivery model, which is becoming common with increasing frequency.

For instance, if you're headquartered in a location where hiring people is inherently difficult, then it would not be a great decision to purchase a new SIEM and try to run it, because you're not going to be able to easily hire the team you'll need. If you're concerned about data and data residency or are in a heavily regulated industry, then compliance requirements need to play into your evaluation. A CIO will be best prepared to define such requirements with the collaboration of the right expert stakeholders.

FOUR

Choose a security partner who will understand your unique business needs.

One of the most important considerations for any potential security partner should be whether your partner can support your ability to stay on top of the market. You should have confidence that you can keep pace with the changes in the threat landscape, vendor base, technology, and the way technology is used. Transformation is continuous, so having a partner to strategically advise you on changes will help you stay on track, securely.

Decision makers who are not satisfied with their chosen security partner usually say it's because the third party does not fully understand the business or critical assets and fails to contribute actionable insights. A third party may be handling operations, but they are not adding value or delivering the business context that is desired from a security partner.

Knowing this, look for an integrated partnership in your search for security support. The emphasis will shift from outsourced security focused on metrics and SLAs to continuous improvement. Here are some things you can look for in order to determine an effective security partner for your organization:

- **They can articulate the value they bring relative to your business objectives** - This requires that your organization share your objectives with potential partners.

- **Proven experience -** Beyond understanding a sole characteristic such as industry, they should understand your industry, size of organization, type of business, desired identity, and how all these factors come together to develop your threat horizon.
- **A strong resume -** They need to have proof points on how the value they propose to bring can be executed.
- **Business ethos alignment -** A security partner needs to align and compliment organizational ethos and culture. They're an extension of your company; not a side line player.
- **They will enhance your posture and improve your security maturity -** The services they're providing to you will do more than check a box. They'll enable your business to innovate while providing you with an improved security posture.
- **They can integrate their security processes and playbooks into your business and tailor the processes to your operations -** The on-boarding of a new security partner requires a number of workshops between the two organizations to refine processes and find a middle ground of working together operationally and in a standardized and repeatable way.

FIVE

Create a culture that allows for rapid innovation while managing risk intelligently.

Balancing risk while innovating is critical. You can go into any new vendor partnership with the best of intentions and the utmost readiness, but you'll still need a reasonable timeframe for learning and adjusting. Do not maintain the view that your transformation is incomplete and wait to reach out to a security partner. Start now to shorten the window of vulnerability and exposure. You must begin somewhere. Implementing even a part of the necessary foundational controls is necessary even though your business is changing.

Secure digital transformation starts with a culture which encourages innovation with security in mind; security should be built in, not bolted on at the end. Often times, involved subject matter experts aren't necessarily experts at security, which is why it's a good idea to engage a security partner who offers the expertise that you're lacking.

56%

of executive leaders say they are unprepared for the pace of change within digital transformation

51%

say they will struggle to meet changing customer demands – Dell

49%

of enterprises are building security and privacy into all devices, applications, and algorithms as a transformation tactic

Ensure mutual transparency of business objectives. Security advice should be informed by desired business outcomes.

Finally, make sure there is a middleperson between the business and security partner to facilitate coordination. It's your best bet for ensuring continuous optimization of services to align with changing business priorities.

Want to learn more?

Click on the links below to continue learning:

WHITEPAPER

Board-Level POV: Negotiating Need to Achieve Acceptable Security Risk

WHITEPAPER

When to Partner with a Managed Security Services Provider

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.