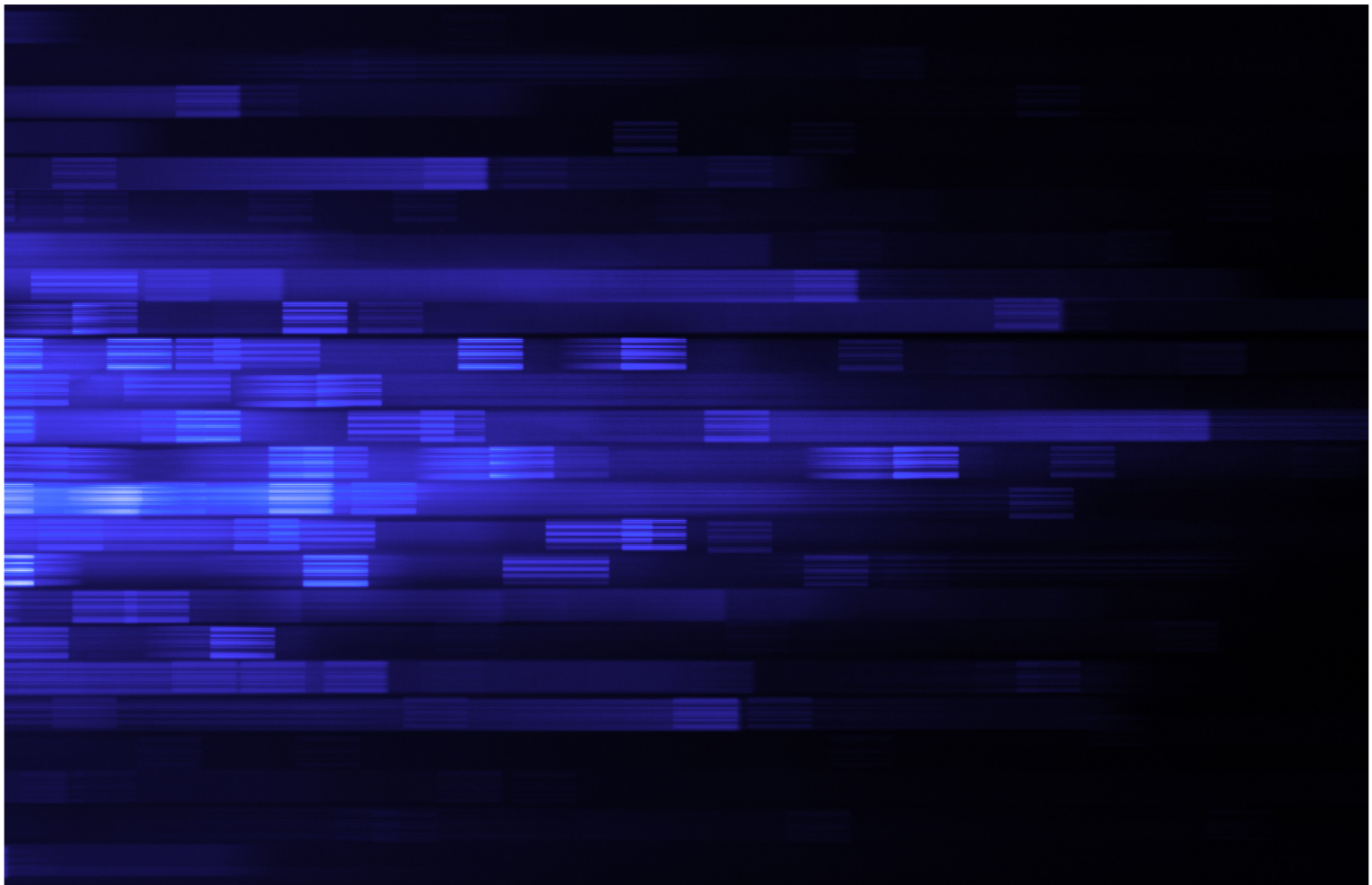


WHITE PAPER

# Four Steps to Developing a World-Class Security Program

The discrete layers and levels of a world-class security organization and program, and how organizations can take advantage of services from Secureworks™ to support their progress toward world-class status.

Secureworks®

**While security threats and vulnerabilities continually evolve, one thing remains constant: organizations need to employ the right mix of people, processes and technology to ensure the highest levels of security.**

Yet the reality is that even organizations that spend inordinate amounts on their security programs can always improve. A report by McAfee and the Center for Strategic and International Studies (CSIS) revealed that cybercrime cost the world between $445 and $608 billion in 2017. That is $100 billion more than the minimum worldwide cost estimated for 2014.[1]

## Adopt a Proactive Security Stance

While a necessity, very few organizations are proactive about putting in place a security framework. Many organizations find themselves in reactive mode, addressing security issues as they arise. That's because no single organization can cover every facet of information security, yet many try. This approach also leaves fewer resources for day-to-day operations. It's akin to a ship springing new leaks the moment one is plugged up because no one on board has the experience, skills or funding to make the ship seaworthy.

**A reactive security approach is all too common, even though the question is not if a company will suffer an incident but when.**

In the business world, the lack of comprehensive, proactive approach means that security programs and a security architecture are usually only developed once the organization is successfully attacked. The data-breach scenario noted above is a perfect example – an organization can only operate so long with security vulnerabilities before experiencing one that is detrimental on a significant level.

In fact, very few organizations adapt their security stance and measures as rapidly as needed. If companies spending hundreds of millions per year on IT security can be breached, it's a sure sign that every organization is vulnerable. That said, by adopting a proactive stance, organizations minimize the likelihood of suffering a breach – or at least increase the chances of discovering breaches before they lead to a substantial, negative impact.

***"Many organizations need to evaluate their digital risk and focus on building resilience for the inevitable," said Sean Joyce, PwC's US Cybersecurity and Privacy Leader.***

**44%**

of the 9,500 executives in 122 countries surveyed by the 2018 GSISS say they do not have an overall information security strategy.[2]




Secureworks

## Step One to World-class Security

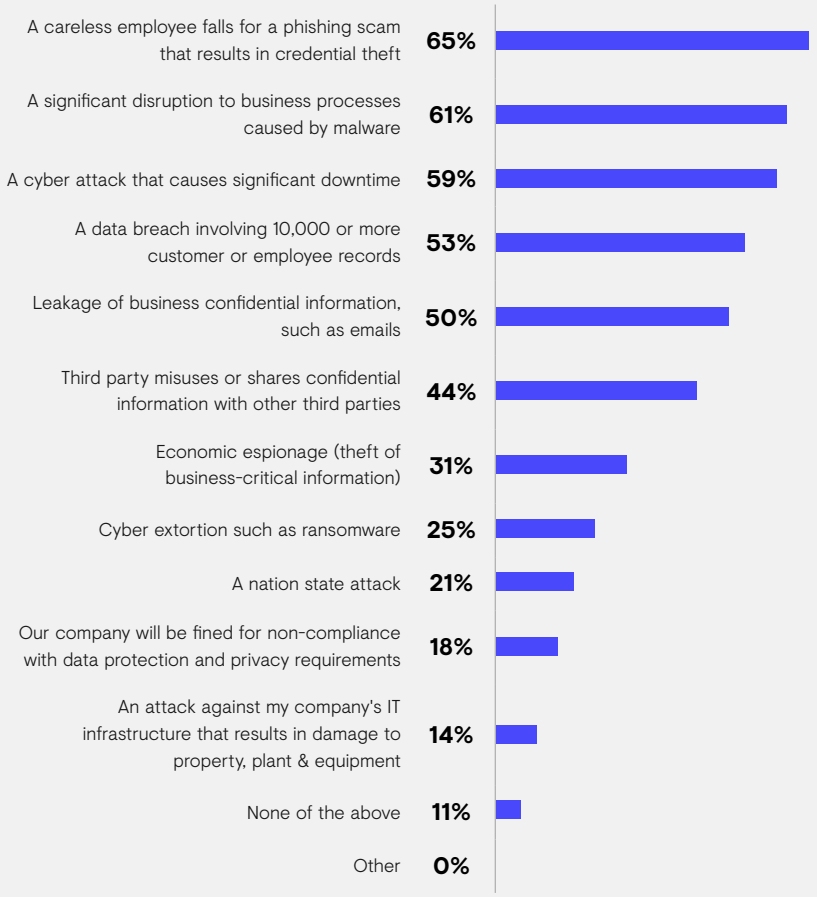
### Align Security with the Business Strategy

Every company has different security needs because they are each protecting unique assets, serving unique customer and user bases, and applying different amounts of resources to security. Yet the bottom line is that security efforts should be working to enable the business instead of hindering it. Many organizations need to prioritize this initiative. CEOs worldwide identify cyber threats as the business threat of greatest concern. US CEO respondents go further by ranking cyber threats as their greatest overall worry, ahead of over-regulation, geopolitical uncertainty and terrorism.[3]

With that in mind, the first step for any organization is to figure out what is important to the business, what needs protecting and why. It doesn't make sense to deploy any security measures or technologies without first understanding this. 67% of respondents believe their companies are more likely to fall victim to a cyberattack or data breach in 2018, so determining security priorities should be top of mind.[4]

***In its annual survey, information security professionals believe that 65% of credential theft will be due to a careless employee falling for a phishing scam — even more likely than a malware attack, a data breach or a cyberattack.[5]***

**What do you predict will happen to your organization in 2018?[6]**
*More than one response permitted*



**Organizations should:**

- Identify the assets that are required to conduct uninterrupted business or that will lead to the greatest financial losses if compromised
- Determine which of those business-critical assets are most attractive to hackers
- Prioritize protection and reaction plans around those assets

Hand in hand with this, all parts of the organization need to acknowledge that security is not an IT requirement – it's a business requirement. To nurture a true partnership between IT and the business, the security team must expand its relationships beyond the confines of the IT group and include colleagues in marketing, sales, HR and other areas of the business in security discussions.

## Step Two: Get a Pulse on Where the Organization Stands

Next the business must understand its current security capabilities – what the organization is doing right and where it faces gaps. That said, security is a journey, not a destination. As such, the organization must continually adapt its approach and architecture according to areas of greatest risk, as outlined in the previous section. Knowing its capabilities and limitations allows an organization to focus on the most important areas that pose the greatest levels of risk to the business.

## Step Three: Design and Build the Security Architecture and Team

Once an organization understands the areas of greatest risk, its capabilities and the people, process and technology it takes to mitigate that risk, it must put in place a fitting security architecture and team to manage that architecture. There's no silver bullet for securing an organization – a security team can't just apply a certain standard or simply employ SANS top 20 security controls and adequately protect the business. In fact, if an organization has aligned security with the business, applying one standard or unrelated standard won't address all its needs. The architecture should be designed to protect all assets and data, with tiered security based on the value and priority of those assets and data.

This tiered approach not only helps the organization prioritize its security focus and spend, it also proves useful when building a business case for elevated security measures. Let's say the cost in time and resources for a comprehensive, blanket security plan is $1,000,000, but the cost to apply security to highly vulnerable "Tier One" applications and data is 50% of that amount. It may be difficult to secure the million-dollar budget amount but possible to get approval for $500,000.

***Other top concerns affecting potential data breaches include:***

**61%**

A significant disruption to business processes caused by malware

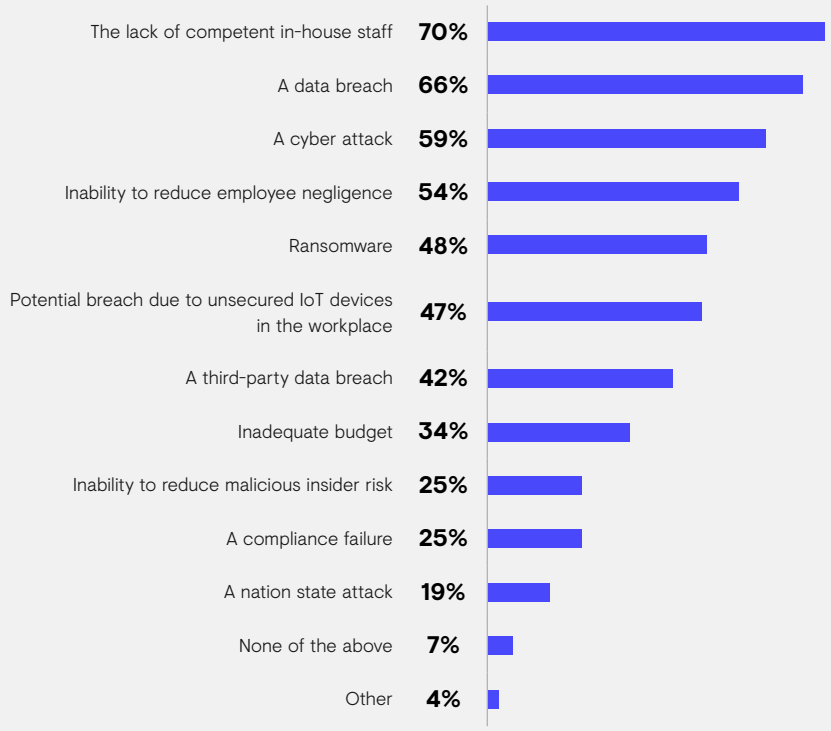
**59%**

A cyberattack that causes significant downtime

**53%**

A data breach involving 10,000 or more customer or employee records[7]

**Which of the following threats do you worry most about in 2018?[8]**
*More than one response permitted*




***The human factor is the top security threat, with 70% of CISOs calling "lack of competent in-house staff" their number one concern and 65% stating "inadequate in-house expertise" as the top reason they are likely to have a data breach.[9]***

At the same time, the architecture's design should take into account the business roadmap. For example, if the company intends to acquire companies in the next 3-5 years, it needs a scalable architecture that can absorb the needs of those companies.

It's also critical to bring on resources to address the gap in capabilities identified above and the variety of security scenarios the organization may face. These resource requirements might include people, process and technology.

## Step Four: Assess the Organization's Security Program Maturity

With a firm understanding of the planning and elements that comprise a world-class security program, next determine where the organization falls on the maturity scale.

| | Completed | In progress | Not started but plan to | No plans |
|---|---|---|---|---|
| **Align Security With Business** | | | | |
| Identify business-critical assets | ☐ | ☐ | ☐ | ☐ |
| Determine which critical assets are likely targets | ☐ | ☐ | ☐ | ☐ |
| Prioritize protection and reaction plans | ☐ | ☐ | ☐ | ☐ |
| **Determine Current Security Stance** | | | | |
| Document security capabilities | ☐ | ☐ | ☐ | ☐ |
| Identify security gaps | ☐ | ☐ | ☐ | ☐ |
| **Design and Build Security Architecture and Team** | | | | |
| Designed to protect all assets and data | ☐ | ☐ | ☐ | ☐ |
| Account for value and priority of assets and data | ☐ | ☐ | ☐ | ☐ |
| Supports the organization's business roadmap | ☐ | ☐ | ☐ | ☐ |
| Secure resources to address capability gaps | ☐ | ☐ | ☐ | ☐ |

## Confidently Evolve by Tapping into Security Expertise

By filling out the assessment table, organizations will understand where they stand – and gain an idea of what is needed to attain world-class security status. That said, some security leaders might feel unsure how to elevate their programs and architecture to world-class levels. Even if they know the necessary steps, they may lack the skills, experience or time to spearhead this initiative. In some cases, IT security may be clear about what people, processes and technologies to deploy, but the executive team wants the assurance of someone with an outside perspective. For these reasons, numerous organizations engage Secureworks, taking advantage of its Security Architecture Assessment Services and Security Architecture and Design Consulting.

Secureworks' consultants can audit to identify and prioritize critical assets and data based on value to the business. This includes inventorying, classifying and assigning value to all assets and data. They can also assess an organization's current security stance/posture to identify weaknesses/gaps across people, processes and technology. This requires an assessment of how well the organization addresses the five key elements of identify, protect, detect, respond, and recover. It also involves an evaluation of how well the organization is performing or can perform the activities required to achieve its security goals as aligned with business objectives. By understanding what the organization is doing right and doing wrong, Secureworks can outline the organization's current risk and architecture profiles. After conducting an assessment, Secureworks' consultants develop a comprehensive, strategic roadmap designed to align with the organization's current and future business needs. This roadmap outlines how the organization can evolve from its current security position to the ideal security stance. It also serves as a blueprint to helping protect key assets and satisfy regulatory requirements.

Secureworks can also design a security architecture that enables this evolution, using a modified version of the NIST cybersecurity framework as the foundation. This framework spells out all key security elements and allows organizations to assess themselves against all domain security functions and categories and sub-categories and identify gaps.

***Secureworks can help implement, manage and upgrade the organization's security architecture over time. By continually updating and revisiting the security roadmap and architecture, Secureworks' consultants help ensure the organization is adequately protected against emerging threats and security issues over time.***

## Conclusion: It's Time to Advance Your Security Organization

No organization can minimize the impact of security vulnerabilities without aligning its security strategy with its business strategy. World-class security requires a methodical approach and clear plan to build security around the business and evolve security over time.

According to PwC, "Leading companies today are rethinking the role of information security in their organizations. They realize that in a digital world, cybersecurity is the key to safeguarding their most precious assets—intellectual property, customer information, financial data, and employee records, among others. But far more than a defensive measure, companies also know that cybersecurity can better position their organization with business partners, customers, investors, and other stakeholders."[10]

Organizations shouldn't let pride come before the fall. If instead they acknowledge that they face gaps in capabilities and engage an organization like Secureworks, they can plug security holes and gain the capabilities needed to shore up protection. This enables them to minimize the impact of security issues while freeing in-house resources for daily operations. In fact, by calling upon Secureworks, organizations can rapidly improve their security posture both today and in the future and seize a competitive advantage.

Sources:

[1] "Economic Impact of Cybercrime - No Slowing Down," McAfee - Feb. 2018

[2] PwC, 2018 Global State of Information Security Survey® (GSISS)

[3] PwC, 2018 Global State of Information Security Survey® (GSISS)

[4] Ponemon Institute, 2018 CISO Survey – Jan 2018

[5] Ponemon Institute, 2018 CISO Survey – Jan 2018

[6] Ponemon Institute, 2018 CISO Survey – Jan 2018

[7] Ponemon Institute, 2018 CISO Survey – Jan 2018

[8] Ponemon Institute, 2018 CISO Survey – Jan 2018

[9] Ponemon Institute, 2018 CISO Survey – Jan 2018

[10] PwC, Cybersecurity: The new business priority, http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.html




Secureworks®

Secureworks®

## Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™


### 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
www.secureworks.fr

**Germany**
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

**United Kingdom**
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

**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
www.secureworks.com.au

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