Many organisations are stuck in a middle stage of [security] maturity...Only 43 percent of respondents say their organisations’ IT security budgets are adequate and most security programmes are only partially deployed.

– Ponemon Institute

**Adopt a Proactive Security Stance**

While a necessity, very few organisations are proactive about putting in place a security framework. Many organisations find themselves in reactive mode, addressing security issues as they arise. That’s because no single organisation 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 a comprehensive, proactive approach means that security programmes and a security architecture are usually only developed once the organisation is successfully attacked. The data-breach scenario noted above is a perfect example – an organisation can only operate so long with security vulnerabilities before experiencing one that is detrimental on a significant level.

In fact, very few organisations 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 organisation is vulnerable. That said, by adopting a proactive stance, organisations minimise the likelihood of suffering a breach – or at least increase the chances of discovering breaches before they lead to a substantial negative impact.
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 organisations need to prioritise this initiative. In its 2015 global survey of information security, PwC found that only 59.75 percent of organisations have aligned their information security strategy to the needs of the business.2

With that in mind, the first step for any organisation is to figure out what’s 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. Yet the PwC global survey shows that only 54 percent of organisations run programmes to identify their sensitive assets, and just over 63 percent classify the business value of their data.

Organisations 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
• Prioritise protection and reaction plans around those assets

Hand in hand with this, all parts of the organisation 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.

The average total organisational cost of all types of data breaches globally has increased 23 percent over three years. In addition, the cost of each lost or stolen record increased 15 percent year-over-year.

– Ponemon Institute
2015 Cost of Data Breach Study: Global Analysis

While the majority of IT security staff view minimising downtime as the primary security objective, corporate leaders believe it is more important to improve the organisation’s overall security posture.

– Ponemon Institute

2 http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml
Step Two: Get a Pulse on Where the Organisation Stands

Next the business must understand its current security capabilities – what the organisation is doing right and where it faces gaps.

That said, security is a journey, not a destination. As such, the organisation 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 organisation 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 organisation 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 organisation; 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 organisation 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 organisation prioritise 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 percent of that amount. It may be difficult to secure the million-pound budget amount but possible to get approval for £500,000.

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 three to five 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 organisation may face. These resource requirements might include people, process and technology.

In its annual survey, PwC found that just over 55 percent of companies have an accurate inventory of where personal data for employees and customers is collected, transmitted and stored.³

³ http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml
**Step Four: Assess the Organisation’s Security Programme Maturity**

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

<table>
<thead>
<tr>
<th>Completed</th>
<th>In progress</th>
<th>Not started but plan to</th>
<th>No plans</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Align Security With Business</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify business-critical assets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine which critical assets are likely targets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prioritise protection and reaction plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Determine Current Security Stance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document security capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify security gaps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Design and Build Security Architecture and Team</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designed to protect all assets and data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account for value and priority of assets and data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports the organisation’s business roadmap</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure resources to address capability gaps</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Availability varies by region. © 2016 SecureWork, Inc. All rights reserved.

www.secureworks.com
Confidently Evolve by Tapping into Security Expertise

By filling out the assessment table, organisations 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 programmes 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 organisations engage SecureWorks, taking advantage of its Security Architecture Assessment Services and Security Architecture and Design Consulting.

SecureWorks’ consultants can audit to identify and prioritise 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 organisation’s current security stance/posture to identify weaknesses/gaps across people, processes and technology. This requires an assessment of how well the organisation addresses the five key elements of identify, protect, detect, respond and recover. It also involves an evaluation of how well the organisation is performing or can perform the activities required to achieve its security goals as aligned with business objectives. By understanding what the organisation is doing right and wrong, SecureWorks can outline the organisation’s current risk and architecture profiles. After conducting a full assessment, SecureWorks’ consultants develop a comprehensive, strategic roadmap aligned with the organisation’s current and future business needs. This roadmap outlines how the organisation can evolve from its current security position to the ideal security stance. It also serves as a blueprint to 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 organisations to assess themselves against all domain security functions and categories and sub-categories and identify gaps.
Conclusion: It’s Time to Advance Your Security Organisation

No organisation can minimise 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 organisations. They realise 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 organisation with business partners, customers, investors, and other stakeholders.”

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

For more information, call +44 (0)131 260 3044 to speak to a SecureWorks security specialist.

www.secureworks.co.uk

---