cyber_reveal

Becoming the Security Team Your Business Needs

BAE SYSTEMS

Introduction

Cyber security is often considered to be a technical problem to be handled by technical people. But, the risks have increased as business reliance on information technology has grown exponentially. The risk of cyber attacks and their impact on business is now one of the most important threats to the safety and sustainability of most companies.

As a security professional, you may be invited to business conversations, but that doesn't automatically mean your opinions will be understood, considered relevant and acted upon.

The security function is constantly evolving. Gone are the days of sharing the number of alerts and volume of malware you have detected. Today, it is vital to have the right information to describe the problems you face and suggest solutions aligned to the business in terms of risk.

How can you integrate the security function into the business and educate, advise, and influence activities with cyber risk implications?

Common Issues Facing Security Teams

Demonstrating meaningful, ongoing, business risk reduction

The threat landscape is in constant motion. The threat actors and their favorite techniques are evolving. Your organization is changing, both in terms of its infrastructure, the tools it is using, and its business strategy. As such, it is more important than ever to understand how threats can affect day-to-day operations and how to relay that information to business leaders.

Ensuring access to skills and experience

There is a massive skills shortage in cyber security; which makes hiring and retention an issue. You can't overload your team with menial tasks. If you are giving your team dull and repetitive work because you don't have the right tools in place, you'll lose them to more interesting, better paying opportunities.

The challenge is getting the right-sized team appropriately tasked – not overloaded, but doing meaningful, interesting work.

Demonstrating and maximizing ROI on security investments

There is no shortage of security devices out there. They can supply you with a lot of information but relating that into actions to take can be difficult. You might have put in an email security device, but unless you are measuring what malware is hitting your company and see a corresponding reduction in alerts, then how do you measure its success?

Demonstrating ROI on managed services, one of your larger expense areas, is difficult if your reporting doesn't support it. Having business relevant reporting is key to bridging the gap between security and business metrics.

So, how do you solve these problems? This is driven by the kind of security team you are.

Complicating Factors for Security Teams

Security needs to become more strategic, relevant and integrated into decision making. However, businesses still struggle with how to view cyber threats not simply as technical, but as critical risks. Is this the fault of the business or the security teams?

The ability to have a shared perspective is critical. Security teams need to express themselves in business terms and metrics in order to become a strategic player across the enterprise.

Across the board there are two types of security functions:

Driven by technology

Most security teams tackle issues piecemeal as they deploy and employ point solutions for point problems, while reporting on the effectiveness of the security architecture. You may be great at understanding the threat landscape and managing the effectiveness of your program. You are also comfortable in assessing and implementing security technologies to protect the business.

Driven by business risk and delivering business value

Security teams who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the business. Having the ability to communicate in terms of business risk allows increasing relevance and support from stakeholders including the board.

Creating a strategic framework of security, risk awareness and cyber risk resilience delivers a common language for business unit leaders and security teams. This encourages business and cyber security alignment and allows for faster innovation.

It also makes the process easier to educate, advise and influence activities with cyber risk implications.

How do you change the conversation from **your** problems to solve to the **organizations** problems to solve? How do you become business relevant?

Leaders within your business are wrestling with their own priorities related to new products and markets, mergers and acquisitions. They are not immediately or obviously related to technology or security, but they have important cyber risk implications. A main objective for the security team when interacting with key stakeholders should be to become a trusted advisor who proactively helps illuminate these issues.

Tips for Becoming the Security Team Your Business Needs

Cyber risk is a business issue that is challenging to articulate. To help make the conversation more relevant and relatable, here are three tips which can help turn information into action:

1) Define threats

Identify who is attacking the company, industry and peer organizations. Have practical examples of the hard lessons others have endured. Explain news events and developments, such as high-profile data breaches or cyber security trends, and explain how they might impact your organization. This includes business disruption, delays in product to market, regulatory fines and reputational damage.

2) Tell the story of cyber risk

Tell the story of the current threats and risks. What are the top business challenges? How do these relate to your mitigation controls and detection coverage? What are you doing well and what needs improvement? What management actions do you and the team need to undertake to support current business challenges?

3) Combat Risk

What is your security program maturity? Be careful to not over use this term, instead detail your organizations readiness to meet the challenges and mitigate the risk. Hiding behind security terms won't resonate. After all, what you are describing is a situational analysis and competitive comparison against the threat landscape, attacker ability and industry peers.

Need help achieving business relevance? Tailor the right mix of managed security and advisory services to support your in-house capability with **cyber_reveal**.

cyber_reveal

Technology that detects. People that defend.

cyber_reveal by BAE Systems is a comprehensive suite of technology and services that bring clarity to your cyber security.

The cyber_reveal suite encompasses cyber risk services, threat intelligence, managed threat services, device management and incident response. Our technology is tailored to your business, allowing you to understand, detect and effectively respond to threats, reduce business risk and improve the return on your security investment.

cyber_reveal combines advanced technology with leading cyber security experts to defend commercial organizations of any size.

BAE SYSTEMS

Contact Details

US: +1 (703)848 7000
UK: +44 (0) 1483 816000
AUS: +612 9240 4600

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com I W: baesystems.com/cyberreveal

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai