SOPHOS

Cybersecurity Blueprint: Assessing Your Organization's Risk

Cybersecurity typically falls on the shoulders of an organization's IT team. But intelligence experts will tell you it's not just an IT problem: it's a business problem. At Sophos, our expert-led threat response team uses a proven framework that helps you holistically address cybersecurity across the organization.

UNDERSTANDING YOUR CYBER RISK PROFILE

Sophos has organized what is needed to improve your cyber risk profile into four unique areas. They are as follows:

- **Organizational DNA:** Operational policies, organizational culture and personnel procedures
- **Cyber Insurance:** Financial impact of exposure based on current cyber liability coverage
- **Legal:** Legal liability related to security, privacy, and data accountability
- **Capabilities:** Technology, people and processes in place to manage, detect, and respond to cyber threats

Answering the critical questions listed below will help you gain a comprehensive and foundational overview of what's required to build or improve your cybersecurity program. This forward planning can include conducting policy reviews, developing breach preparedness strategies, and practicing enterprise-wide cyber hygiene.

Organization DNA

Take a hard look at your company's culture, risk tolerance, operations environment, and breach preparedness by addressing these topics:

Culture

- How would you describe your corporate culture?
- What is your company's overall risk tolerance?
- Are employees permitted to work remotely?

Operations

- Is your operational environment on-prem, in the cloud or a hybrid of the two?
- What types of sensitive data do you collect, handle or store? Where are these located?
- How would you describe your business-critical applications?

Threats

- What are the top security threats to your organization?
- Do you feel that your data and critical infrastructure is a greater target for ransomware, insider threats or nation-state attacks?
- How would you rate your company's breach preparedness?

Cyber Insurance

Answering the following questions will help provide clarity around your cyber risk policies and shine a light on how you and your breach response providers align to those policies:

Policy

- Do you have a cyber liability insurance policy in place?
- What coverages are included?
- What is your policy limit and retention?

Alignment

- Are you in alignment with your cyber coverage application responses?
- Have you added any new security controls?
- Has your total record count changed?

Breach Response

- Which breach response providers are included in your policy?
- Do you know of any potential conflicts? If so, what are they?
- Can you work with "off-panel" vendors?

Legal Response

Gain clear visibility of what protections are in place and any other compliance needs. From contracts to privilege access to breach communications, here's what you need to consider:

Contracting

- Do all contracts go through a standard data security review?
- Is there clear demarcation of data custodianship and security response?
- Has the organization identified high-impact vendors (third parties)?

Privilege

- Do you have access to a data breach coach?
- Organizationally, has the moment been defined as to when an incident should be considered a breach?
- Is there company-wide agreement as to which breach scenarios will require public disclosure?

Compliance

- What regulations/requirements does the organization currently adhere to?
- In the event of a breach, is customer notification part of the response?
- What specific actions must be taken per state regulations?

Capabilities

Consider these questions as you shore up security tools, elevate incident response plans, and uncover critical process gaps:

Environment

- Are security tools/controls deployed across the entire environment?
- Are the selected tools appropriately configured to meet the evolving needs of the organization?
- Have they been integrated for maximum efficacy (i.e.: synchronized security)?

Preparedness

- Have you identified which sensitive data is being stored and where it resides?
- Do you have a formal incident response plan in place?
- Have you conducted tabletop exercises to identify process gaps in emergency situation responses?

Incident Response

- Are on-prem, in-the-cloud and hybrid environments monitored 24/7?
- Can you detect sophisticated (new and novel) attacks on sensitive data assets?
- Are you able to respond to and neutralize threats prior to a potential breach?

DON'T BUILD A BLUEPRINT IN A VACUUM

This framework clearly illustrates that building a solid cybersecurity plan is not just the concern or responsibility of an organization's IT team. Carefully addressing the questions above enables you to look more holistically across the organization and bring key stakeholders to the conversation to design the best path forward toward improving your cyber risk profile.

The Sophos Cybersecurity Risk Organization Blueprint is just a starting point to begin the conversation.

We can facilitate guided discussions and help you put together a business plan to improve your cyber risk profile for the long term. Simply email our team at nasales@sophos.com to learn how Sophos can support your security planning needs whether it is to build or improve your cybersecurity program.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2021-04-13 (MP)