RAPID7

Implementing Protection Level Agreements for Greater Cybersecurity Effectiveness

Rethinking risk to operationalise cybersecurity

Contents

Background

Measuring security effectiveness continues to be a common challenge. Unfortunately, many organisations' fragmented approach to cybersecurity often goes unnoticed unless it's highlighted during customer engagements. The problem is compounded by the need to consider risks differently and relative to each environment and/or use case – public cloud, private cloud, on-prem, third parties and virtual machines, to name a few.

Gaps continue to increase between departments due to unfocused cybersecurity outcomes, inconsistent measurement, undefined priorities, and value drivers. When cybersecurity is separate from the traditional business process, it results in fragmented business units and raises operational costs without reducing the level of risk.

The challenge

Failure to measure security effectiveness, gaps, and silos between stakeholders creates several challenges often invisible to the business:

Cause	Effect
New projects	**1.** Limited focus on security objectives or scope **2.** Lack of alignment between teams and stakeholders **3.** No clear direction on what needs to be executed **4.** Limited understanding of costs, resources, and timing to develop better business cases
Performance problems	**1.** Poor understanding of changes amongst stakeholders **2.** Lack of visibility if security is becoming part of the business process **3.** Difficult-to-identify connections between symptoms and causes **4.** Little validation if an implementation plan is complete and effective **5.** Lack of data and evidence to show or effect change **6.** No clear way of determining if security improvements are effective **7.** Confusion when measuring ROI
Lack of alignment between business functions or teams	**1.** Differing views on what needs to be achieved **2.** Lack of a common approach and shared objectives **3.** No line-of-sight between purpose and activity **4.** No clear way of translating technical items to business stakeholders
Team challenges when implementing a plan	**1.** Risk is not reducing **2.** No way of tracking external change or technical data **3.** No common way to move from a Current Operating Model to a Target Operating Model

Additional potential issues

- Cybersecurity is a business decision, not a technical decision, but is being addressed by technical data
- Cybersecurity silos need to be addressed, and technical data is not solving the problem
- The need to translate cybersecurity into business value
- Leadership and executives need to gain control and ownership of cybersecurity – this ensures business context can help to provide the appropriate level of investment
- Business stakeholders (executives, board members, investors) require a non-technical way to measure the effectiveness and maturity of cybersecurity
- Most businesses have no clearly defined business cybersecurity metrics
- All business functions measure cybersecurity differently

What is a Protection Level Agreement?

A Protection Level Agreement (PLA) is an agreement between two or more parties which specifies security criteria a provider promises to meet while delivering a service. It comprises a set of non-technical standards that are jointly created and agreed upon in order to raise cybersecurity awareness.

Measuring the performance of PLA is done by setting metrics with corresponding Protection Level Objectives (PLOs) and supporting Key Performance Indicators (KPIs). This can be a legally binding formal or an informal "contract" (for example, internal department relationships). The agreement may involve separate organisations or different teams within a single business.

Benefits of a PLA

Reduces security risks	Implementing PLA will dramatically decrease the cycle times (time to resolve risks)
Facilitates communication	Business functions will be able to set business expectations in two ways: 1. They can refer to the PLA document for definitions of priorities and the maximum time business functions have to identify or resolve risks 2. The business can track performance reports to inform stakeholders how the company or functions are performing non-technically
Negotiated and mutually accepted	When jointly creating a PLA, all parties will more readily accept its requirements
Defines procedures	Procedures can be created that are tied to the PLA and makes cybersecurity a part of the business process
Questions or disagreements	The PLA can be used as a written reference
Sets non-technical security business standards and objectives	It demonstrates to the organisation how business functions and cybersecurity are going to address and manage risk. It ensures business functions or teams are ready to measure and report on performance and cybersecurity effectiveness

Example PLA

<table>
<tr><td><b>KPI / PLA name</b></td><td>Protection Level Agreement for Critical Vulnerabilities</td></tr>
<tr><td><b>Description</b></td><td>All stakeholders and employees acknowledge that critical vulnerabilities will be addressed within a set period</td></tr>
<tr><td><b>Scope</b></td><td>
<table>
<tr><th>Environment</th><th>Time to resolve (KPI)</th></tr>
<tr><td><b>Internal Cloud Environments</b></td><td>30 days</td></tr>
<tr><td><b>Customer Cloud Environments</b></td><td>5 days</td></tr>
<tr><td><b>Internal Servers</b></td><td>60 days</td></tr>
<tr><td><b>External web facing assets (DMZ)</b></td><td>10 days</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td><b>Measurement</b></td><td>Monthly reporting against the scoped PLA</td></tr>
<tr><td><b>Data to measure</b></td><td>Rapid7 InsightCloudSec and InsightVM</td></tr>
<tr><td><b>KPI / PLA Owner</b></td><td>CISO and/or Board Members</td></tr>
<tr><td><b>KPI / PLA Target</b></td><td>100% resolution or clearly defined mitigation or business case supporting not meeting the PLA</td></tr>
<tr><td><b>Personas accountable to KPI / PLA</b></td><td>
<table>
<tr><th>Environment</th><th>Persona</th></tr>
<tr><td><b>Internal Cloud Environments</b></td><td>Cloud Opps
Cloudsec</td></tr>
<tr><td><b>Customer Cloud Environments</b></td><td>Product Management
Cloud Opps</td></tr>
<tr><td><b>Internal Servers</b></td><td>Infrastructure team</td></tr>
<tr><td><b>External web facing assets (DMZ)</b></td><td>Infrastructure team</td></tr>
</table>
</td></tr>
</table>

When to use a PLA

There are many reasons why a current Cyber Target Operating Model (TOM) perhaps isn't as effective as it needs to be. Asking straightforward questions of key stakeholders across leadership will yield insights that can help you know when to deploy a PLA and improve the effectiveness of a new PLA.

- Shortly after new leaders or key personnel come aboard
- After a reorganisation of business units or critical teams
- At the time of setting clearly defined PLA goals across the business or between business functions
- When implementing cybersecurity KPIs to measure outcomes, performance, and successes
- Whilst defining your current level of risk across all environments
- At the point of reviewing critical business functions, and defining how they relate to the potential levels of risk
- When struggling to get different business functions to take ownership or resolve security vulnerabilities identified

A Cyber TOM can address issues that stem from answers to these questions. The TOM should be underpinned by solid PLAs – addressing aspects like critical vulnerabilities – and supported by strong KPIs.

The importance of KPIs in combination with a PLA

KPIs allow cybersecurity teams and businesses to measure security efforts. This facilitates the Chief Information Security Officer (CISO) and business stakeholders to leverage KPIs so they can demonstrate the return on investment that comes from security spending. KPIs are also commonly used to raise security awareness across cross-functional teams and vendors.

Including KPIs in cybersecurity awareness training can result in:

- A comprehensive understanding of security threats
- Greater knowledge of the roles of various business units
- Support and influence on business objectives
- Managing performance with greater efficiency
- Stronger employee morale
- Personal employee growth

Using KPIs to enable cybersecurity maturity

To start operationalising cybersecurity using a TOM and PLAs, the maturity of each foundational component of a cybersecurity program needs to be set. Mature foundations will help ensure your business properly leverages cybersecurity and can track the effectiveness of threats and risk management. For each of the TOM foundational components, the requirement is to increase the level of maturity – KPIs can help track this process and make it a success.

Stay prepared

While you're never going to guarantee 100% that you'll be able to stop attacks from happening, being prepared will decide the extent to which an attack could damage your organisation. Attackers will always try to remain one step ahead of any plans or measures you may have in place, so consider how a partner can help you further your cyber resilience, particularly in light of the current lack of skills and resources.

As a partner to many organisations globally, Rapid7 can help guide you through cybersecurity challenges, providing vital expertise and support to your team.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organisations strengthen their security programmes in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web.

We foster open source communities and cutting-edge research – using these insights to optimise our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

Contact Rapid7 to see how we can help you.

RAPID7

NORTH AMERICA:
+866.7.RAPID7
sales@rapid7.com

EMEA:
+44.1183.703500
emeasales@rapid7.com

APAC:
+65.3159.0080
apacsales@rapid7.com