CISO Guide:
MEASURING AND ENHANCING ENTERPRISE CYBER-RESILIENCE

Balbix
CISO Guide: MEASURING AND ENHANCING ENTERPRISE CYBER-RESILIENCE

Executive Summary

Cyber-resilience is a popular term in the cyber security business. According to the most common definition of the word, it is the ability of an enterprise to limit the impact of security incidents and is a broader approach that encompasses cyber security and business continuity management which aims to not only defend against cyber-attacks, but also ensure that the enterprise is able to survive following an attack.

The enterprise attack surface is vast, constantly growing, and poorly understood, and the threat landscape is constantly evolving. Our enterprise networks contain large amounts of insecure software (and hardware) and all this is developed, managed, and maintained by people — making them all entities that are imperfect and fail regularly from a security standpoint. The objective of security teams is to implement mitigations to offer a cyber-resilient enterprise on top of insecure components. This is a tall order.

How is cyber-resilience defined and measured? How are breach risk and cyber-resilience related, and what is the best way to improve cyber-resilience for an enterprise? This paper will answer these questions and shed light on steps you can take to improve the cyber-resilience of your enterprise.

Defining and Measuring Cyber-resilience

Cyber-resilience is the ability of an enterprise to limit the impact of security incidents. In this context, resilience means the preparations that an organization has made with regard to threats and vulnerabilities, the defenses that have been developed, controls implemented, and the resources available for mitigating a security failure after it happens. The inclusion of a deep understanding of cyber risk in strategic planning is an integral part of cyber-resilience.

Cyber-resilience is not an opaque score that is derived from some simple scoring of “n” properties of a network. It is also not a number that you arrive at by answering a set of questions about your network. It is more complicated than that but can be calculated in a reasonable manner from observations of the state of your enterprise and a series of probabilistic mathematical calculations.
To understand the structure of cyber-resilience, let’s consider the graph in Figure 1, which plots the likelihood of breach of a typical enterprise vs effort by the adversary.

The y-axis in this picture is the likelihood of breach, a probability number between 0 and 1. The units on the x-axis are arbitrary and could be measured in a number of different ways, for example, in terms of time spent by the adversary, or number of attempts, or money spent. (In this abstract picture and other visualizations in this article, we take some liberties with mapping multi-dimensional values and functions to 2 dimensions for the ease of understanding.)

The shape of the Likelihood vs Effort curve is consistent with one intuitive notion that all security practitioners agree with — given enough effort, anything can be breached. Every enterprise has a Breach Likelihood vs Effort curve like the one shown in Figure 1. The only difference is where the knee of the curve is on the x-axis, and the slope of the rise from 0 to 1.

Intuitively, you might think that for networks of security-mature companies, like a Fortune 500 bank, the knee would be expected to be well towards the right of the axis. For a smaller, less security mature company, we would expect the knee to be more towards the left (Figure 2). This is largely true. But, there is also a natural entropy in play that tends to move larger, more complex networks closer to the left — everything else being the same, it is easier to break into a network with 10K moving parts than it is to break into a network with 10 moving parts.

An intuitive notion that all security practitioners agree with: given enough effort, anything can be breached.
As you might imagine, this curve is not fixed for your network for all time. As you make changes to your network, the curve changes. The deployment of a new mitigation might push the curve significantly to the right, decreasing the slope. The discovery of a new vulnerability which ends up getting used by cyber-criminals, will move the curve to the left and perhaps make it steeper, until the vulnerability is patched. Given that your network has lots of elements and is under constant change — new devices and users, new applications, new configurations and vulnerabilities, upgrades and patches, this Likelihood vs Effort curve changes on a daily basis (hopefully within a narrow range, like a guitar being played), as illustrated in Figure 3. Without loss of generality, we may assume that the leftmost curve in such a family of curves is the important one for the purposes of risk modelling and estimations.

For another insight into why these curves are shaped the way they are, consider a typical breach. A breach usually begins with one or a handful of vulnerable systems being compromised. This might happen because of an employee being phished, or via a weak password for a system or application, or some unpatched vulnerability. In rare cases, the adversary may use a zero-day exploit to establish this initial beachhead. These initial compromise methods require varying degrees of effort by the adversary, as shown in Figure 4.

After the initial compromise, the adversary is able to jump quickly from system to system, which is why we see the sharp increase in the slope of the graph. Propagation is rapid because a fundamental design goal of our intranet is to enable ease-of-use and collaboration. Once the adversary has a beachhead on an enterprise device, they can use the fast pathways that exist inside the enterprise network to enable high productivity for the legitimate users of the compromised device.
Now, you may have some questions:

- Why is the knee for a network at a certain spot?
- Why do some networks have a gentle slope, while others have a sharp rise from 0-1?
- What is exactly is my risk from cyber breaches today?

To answer these questions first let’s convert this style of plotting to Risk Math instead of Likelihood Math. You may recall that Risk = Likelihood * Impact. This is shown in Figure 5.

In this picture, the x-axis is the same as before—arbitrary units for effort by the adversary, measured in time, # of attempts, or money spent. The y-axis is the impact of a breach. This can be expressed in dollar units, or as a fraction of the revenue or market capitalization of the organization. The shape of the curve is very similar to that of the likelihood curve. One point to note here is that impact itself has three dimensions, availability, confidentiality, and integrity — and we are mapping these three vectors to a single dimension for keeping this discussion simple. Additionally, Impact is also a function of mean-time-to-repair (MTTR), and we are going to gloss over this factor for this discussion.

So, what exactly is my breach risk today? That depends on the threat level AND the state of my enterprise with respect to this threat level. While the threat level is very difficult to know exactly, we might be able to estimate a useful range. This is shown in Figure 6.
As you can see, knowing your breach risk given the threat level is very insightful. In particular knowing whether the threat level is to the left of the knee or to the right. If the threat level is to the left of the knee, congratulations, you are good. If the threat level is to the right of the knee, this is not so good. Perhaps the most concerning thing here is that the slope of the curve is quite sharp, and it is difficult to know if the error in the risk estimation is significant — you could think you are just to the right of the knee, but a small change in the threat level or your enterprise’s state could cause you to be at high risk for a major breach.

It is for this reason that we need to consider the slope and the max value of the Breach Impact vs Effort curve, as shown in Figure 7. These two metrics are the components of cyber-resilience. For a more secure network we want to ensure that small changes in effort by the adversary will not change the risk significantly. We also want to ensure that the maximum impact of a breach is limited.

So, what does cyber-resilience depend on?

As you might expect, resilience depends on the configuration of all your IT assets and the mitigations you have implemented, and the effectiveness of your people and processes who are operating the mitigations. For example, to on-premise infrastructure using network segmentation, 2-factor authentication, advanced endpoint controls, using bastion hosts for network administration, ingress and egress filtering, VPNs, SoC automation — all improve resilience.

For cloud-hosted systems, we have a similar but somewhat different list of mitigations that affect resilience. Likewise, we have different sets of mitigations that are key for impacting the resilience for each type of device, user and applications in your network. You can, in fact, consider that the curve in Figure 7 is the result of the composition of many smaller curves, one for each asset in your enterprise. Unfortunately, again, the composition is not a straight sum but a probabilistic, weighted graphical sum that depends on how your different IT assets are configured and interact with each other.

Cyber-resilience depends on the configuration of your infrastructure, the current controls and mitigations in place, and effectiveness of people and processes operating the mitigations.
Making complex calculations possible

The computation involved in calculating and addressing cyber-resilience is quite complex. The observations that are needed to feed into this math need to be gathered from all the entities in the extended enterprise network — users, assets, applications, their interactions, system and application configuration, human behavior, ACLs, mitigations, the state of all security products and intimate knowledge of the global threat model.

To build such a system, Balbix uses a large number of data points. Using hundreds of observations about indicators of risk from host, network and external vantage points funneled automatically through an AI backend to learn risk-related aspects of the network — including business impact, Balbix BreachControlTM builds a comprehensive and predictive, bottoms-up risk model. The model presents a clear picture of which users, apps and devices drive the enterprise’s overall breach risk — see Figure 8, for an example.

The best way to improve cyber-resilience is to continuously discover and monitor all points in your attack surface, analyze this information to predict likely breach scenarios and take appropriate mitigating steps. The Balbix system can predict critical breach scenarios, help users prioritize security operations and projects, prescribe specific mitigations and best practices, and ultimately improve cyber-resilience.

Let Balbix show you how you can measure and improve your cyber-resilience, and prevent cyber-disasters!