Understanding and Managing Cyber Risk: *A Three-Part Framework*

By Nick Streaker, VP of Technology, Secure Halo

As the infrastructure we rely upon continues to become more diverse and our core business functions become decentralized in the drive to improve efficiency, it's necessary to adjust the optic through which we understand and manage cybersecurity risk.

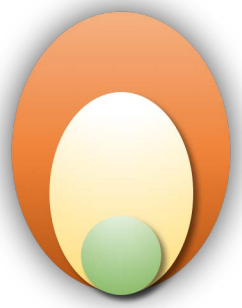
With critical dependencies expanding beyond the sphere of our control, we must posture ourselves in a way that allows us to minimize both our susceptibility to, and the impact of, cyber threats.

At Secure Halo, our experience providing cybersecurity assessments and consulting has shown a simple truth - security is a process, not a product. Though vendors will continue to develop new cutting-edge technology promising to be a panacea for security woes, without addressing the core fundamentals of security, businesses will not be adequately postured to address risk in a meaningful way.

Moreover, in using those tools, many organizations believe that the necessary mechanisms are in place to address their risk. In numerous cases the opposite is found to be true. Without the ability to measure the effectiveness of an organization's security posture, "a best guess" will most accurately describe how risk is being addressed.

This, combined with expanding footprints outside the walls of an organization and the dynamic nature of the threat environment, has led us to view cybersecurity risk through a three-part framework:

1. **What you can control.**
2. **What you can influence.**
3. **What you cannot control.**



Without addressing the core fundamentals of security, businesses will not be adequately postured to address risk in a meaningful way.

It's a simple but powerful approach that is applicable to any organization interested in cyber resilience by expanding its field of view and aligning strategic investments and decision-making to bring outlying elements into the sphere of control. In order to accomplish this, it's necessary to first understand each category.

1 Things You Can Control:

These are traditional methods and mechanisms that can be put in place that generally fall within the Governance, Risk Management, and Compliance (GRC) functions of an organization's security posture.

They include:
- the existing structures to align business goals with security needs
- management and oversight methods to mitigate risks without unnecessarily hindering efficiency
- compliance requirements based on industry vertical

These are the fundamentals from which a culture of security is born. Though these are areas where organizations can have full control, many we've assessed, including very large companies, still lack a cybersecurity governance and management structure.

Even worse, there is often a complete absence of certain fundamental security controls. These shortcomings allow emerging threats, such as ransomware, to be consistently effective despite being relatively easy to prevent.

Ransomware attacks, where a computer or its data is held "hostage" by hackers until payment is made, saw a sharp increase last year. Almost one out of every two participants in a 2016 Osterman Research survey indicated that their organization suffered at least one ransomware attack in the past 12 months, and Beazley Breach Response Services reported clients were the targets of more attacks in July and August of 2016 (52) than in all of 2015 (43).

The prevalence of these attacks is not the point, however. Rather, it demonstrates the failure of organizations to implement simple controls that would both prevent ransomware from occurring, and create a resilient posture to recover with minimal impact.

The concepts of building a solid security foundation and implementing fundamental controls are all that is needed to address many of the threats that are lurking in the dark shadows across the cyber landscape.

Threat actors are clever, but at the end of the day, defending against ransomware is just defending against malware, something you can control.

2 Things You Can Influence:

Areas that are managed as an extension of day-to-day business and the interfaces that extend outside the walls of an organization are those that can be influenced. For example:

- organizational processes for vendor management
- assessment of risk involved with outsourcing services
- articulation of language included in third-party agreements and contracts

Although the services and products themselves fall outside of what your organization has direct control over, you do have the ability - and the responsibility - to shape the security environment in a manner that protects your organization from risk.

According to RightScale's 2016 State of the Cloud Report, 95% of businesses are using cloud services to some degree, which is an area that organizations can directly influence. While it's likely that cloud service providers have built-in security features that exceed the capability of an individual organization, you still need to ensure an in-depth defensive strategy for assets outside organizational ownership and control. Therefore, it is essential that you influence as many of these relationships as possible, instead of relying on their existing, potentially unsecure practices.

Third-party cyber risks should in fact be considered upfront when contemplating shifting the operational control of a critical element of the business, since doing so means you will relinquish some of your own preventative and detective control.

If critical business functions are being outsourced, they can become a single point of failure. This makes applying a security process and security fundamentals to areas that are beyond your control, but not beyond your influence, essential to empowering your organization.

By identifying aspects of third parties' security posture that align with or are in conflict with your own organization's security, you shift from viewing cloud service providers as a potential vulnerability, to recognizing them as an active participant in the improvement of your security posture and lowering your potential risk across the enterprise.

3 Things You Cannot Control:

This category consists of what falls distinctly outside the realm of what we can either control or influence. Among these are unknown future threats against infrastructure. The difficulties we face in assessing risk in a dynamic environment full of uncertainty are the overreliance on the accuracy of our models, and assessing risk through a dangerously narrow optic. We are more inclined to weigh both the accuracy and impact of what IS known more heavily in order to posture ourselves to be resilient against the unknown.

The Internet of Things is a perfect example. The continued increase of interconnectivity of countless products opens the door for new security challenges.

A growing number of devices will have the capability to be connected. Attacks will be leveraged - we've already experienced the massive Dyn Distributed Denial of Service (DDoS) incident – due to the astronomically large number of devices that were not built with security in mind.

The problem does not lie with the devices themselves but rather with their origin and their manufacturers. Business is global in nature. The diversity of global components in manufacturing specifically, cannot be realistically managed.

Instead of looking for regulatory forces nationally to shape the security environment, forces with similar global reach, such as the insurance industry, have the opportunity to change perspectives on how we address risk beyond our control.

The Dyn DDoS attack was successfully executed, impacting a number of high profile companies. Etsy, the peer-to-peer e-commerce website was an exception. While it used Dyn for managed Domain Name System (DNS) service and experienced some delay, it was not crippled as other companies were. Etsy used an additional DNS provider and this forethought created institutional resilience that protected it from the full impact of an attack that was unprecedented in size.

This is a prime example of a company that analyzed its risk in terms of what it can control, what it can influence, and what it cannot control. From there, Etsy implemented a security process to support resiliency, which took a situation from beyond its control and shifted it into an area it could influence - which is the ultimate goal.

Risk is non-linear and experience shows that making extrapolations based on external inputs and historical data is only part of the picture, especially in the ever-changing digital ecosystem. Organizations should focus on making decisions that escalate levels of control and expand zones of influence, resulting in a holistic picture of potential risk.

By viewing security as a process through the optic of what can be controlled, what can be influenced, and what cannot be controlled, the opportunity exists to extend our reach beyond the physical walls of our organizations. This allows us to clearly see the true breadth of the security risks we face, and be in a position to make informed decisions.

Nick Streaker, CISSP, has more than 15 years of experience with leading global security companies. At Secure Halo, he leads technological development and provides cybersecurity consulting to commercial clients and federal agencies.