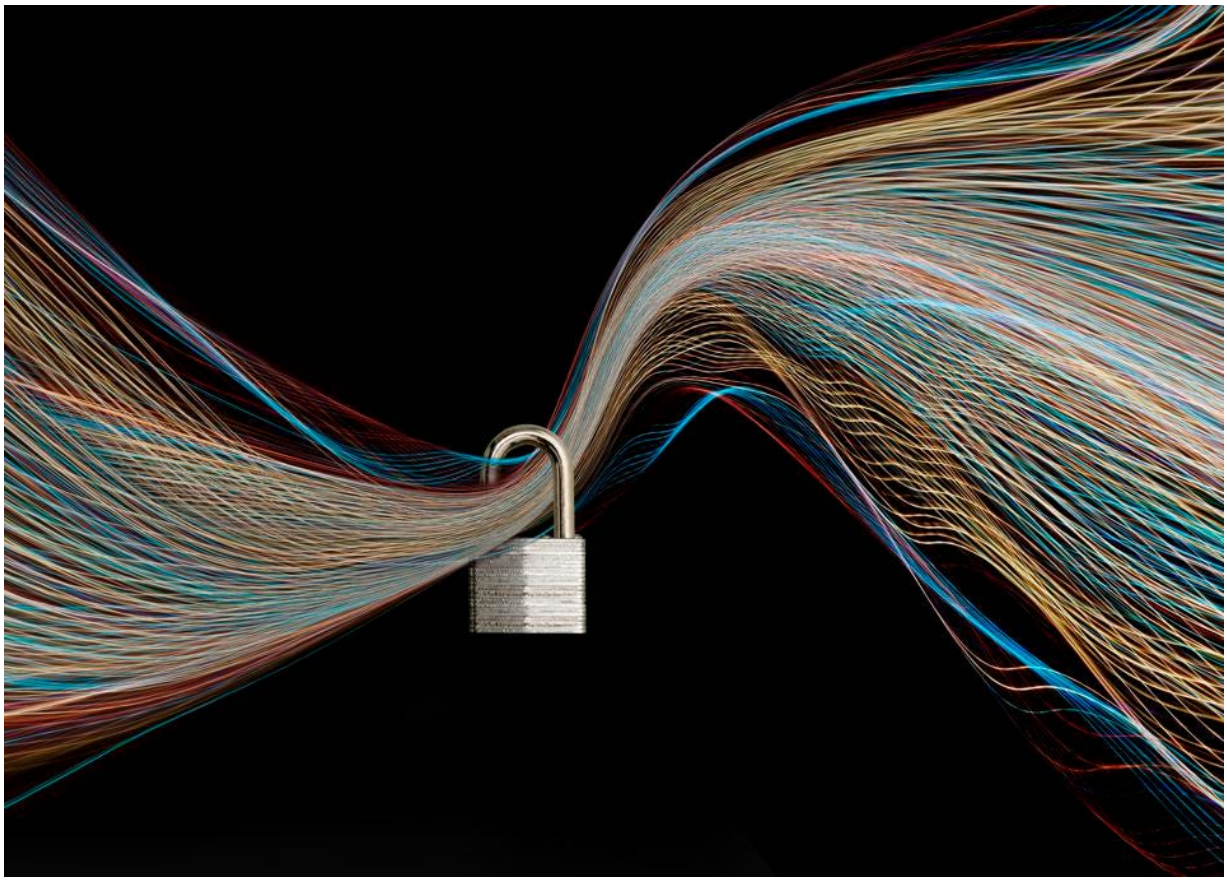
Mar 4, 2022, 09:00am EST | 178 views

A Cyber Risk Management Primer: Identifying Risk, Vulnerability And Threat

Jim Goldman Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Innovation

Jim Goldman, Co-founder and CEO, Trava Security, Inc.



GETTY

The statistics are scary: Cyberattacks continue to rise, with a 125% increase in incident volume year-over-year in the first half of 2021 alone, according to Accenture. A single data breach costs a small business an average of almost

$3 million, according to IBM's 2021 Cost of a Data Breach Report — a 26.8% increase from 2020.

Almost 90% of small and medium-sized business owners believe they are vulnerable to cyberattacks. Yet as few as one in five carries cyber insurance, and a holistic cyber risk management program is far from common.

Businesses know this risk is universal. They know they are unprotected. Why do they fail to act? In speaking with SMB owners and executives around the country, I discovered that for many, there is confusion over what "cyber risk management" actually is, and that confusion is preventing them from taking action.

In many ways, cyber risk management is identical to any other kind of risk management. To introduce the concept of cyber risk management, I often start with a jewelry store metaphor, as I did at the "Cybersecurity Awareness for SaaS Companies" event in October 2021 (here's a snippet).

A jewelry store does certain things to protect its inventory day to day — puts locks on cases and doors, installs security cameras and a safe to store jewelry at night. Those measures prevent the most likely types of loss and must be maintained to continue to be effective. It has store policies and employee rules. The owner or manager checks regularly to be sure the locks and cameras are working, and everyone knows and follows protocol. The store is

insured because no matter how secure it is, unanticipated losses might occur.

That's risk management.

Identifying Risk, Impact And Threat

Identifying the risk, impact, threat, threat vector and threat actor provides the basis for creating a comprehensive vulnerability mitigation and management program — to occur on an ongoing basis since unforeseen threats can always arise. But what is the difference?

Risk is something that *might* happen (e.g., a break-in, a data breach) — you don't know that it will, but it might. But how likely is it? That's the first consideration when calculating risk. The second consideration is impact: How bad will it be for a person or a business if this event occurs?

Impact can often be expressed in dollars (e.g., replacing a window or some stolen jewelry, paying experts to patch the holes in your computer system).

Therefore, risk can often be defined in a dollar amount as well (though not always).

A threat is something someone could do that would compromise the asset that your business is trying to protect (e.g., jewelry, sensitive customer data).

The entry point of that threat is referred to as the threat vector (e.g., an unlocked window, an inadequate firewall) — also called a vulnerability. The person or entity who could do harm (e.g., a burglar, a hacker) is the threat actor.

Establishing A Cyber Policy

Like any other company policy, a company's cybersecurity policy should be stated clearly for employees and other relevant stakeholders (e.g., vendors and contractors). This policy is critically important and should be widely known.

An effective risk management program requires laying out a high-level statement of what you want to achieve: a policy. A policy requires governance — active attention to whether the policy is being adhered to — typically an operations, IT or senior management function.

Policies tend to be broad in scope, voicing a company's commitments and intentions; they are unlikely to change over time. Standards and procedures are policy components that lay out what needs to happen and how.

• **Standards** are the mandatory requirements to satisfy policy objectives — do's and don'ts that will be prone to change as supporting systems and technologies change. New cyber threats are surfacing frequently, so cyber policy standards tend to evolve more rapidly. (In fact, a set of cybersecurity standards that remains unchanged after a year could be a red flag.)

• **Procedures** provide a step-by-step guide for how to implement a standard. Procedures typically change often — not only in response to new threats but as new protocols are developed for addressing ongoing concerns.

Mitigating Controls, Compliance Monitoring And Internal Audit

Beyond successful governance of a policy, businesses can reduce risk by implementing mitigating controls — practices that enhance their primary security measures. For a SaaS company, that could mean endpoint detection and response software on laptops and multifactor authentication.

Compliance monitoring and internal audits allow companies to make sure mitigating controls are properly implemented and to continually check systems, devices and networks against the business's published standards and any other specifications.

If they discover a deviation from the standard, then it is reported as an issue — meaning something that has happened (as opposed to a risk, which you will recall is something that might happen).

Cyber Risk Management Demystified

So that's the primer. Cyber risk management is in fact just risk management that happens to apply to cyber concerns, using the same process and terms:

• Identify risk, impact and threat to your assets.

• Identify the threat vector or vulnerability and the threat actor.

• Establish a policy under governance that contains standards, which could change over time, and procedures, which may change more often.

• Establish mitigating controls (compliance monitoring and internal audit), during which time deviations will be noted and issues (past incidents) reported.

When the once-reluctant SMB owners and executives I talk with go on to discuss their cyber risk management planning process or policies with their employees, I imagine they too might say, "Think of a jewelry store."

Forbes Technology Council is an invitation-only community for world-class CIOs, CTOs and technology executives. *Do I qualify?*

Follow me on Twitter or LinkedIn. Check out my website.

Jim Goldman

Jim Goldman, Co-founder and CEO, Trava Security, Inc. Read Jim Goldman's full executive profile here.