A Broader Role for Cybersecurity Leaders: Enterprise Risk Management

The COVID-19 pandemic offers clear proof that enterprise risk management is not just an exercise, but a crucial government function. To protect their operations and continue to fulfill their public-service missions, governments need robust plans for mitigating a range of potential emergencies.

Robert Huber, chief security officer at Tenable, says cybersecurity professionals should play a larger role in enterprise risk management. He discussed how cybersecurity leaders can contribute to this crucial function in government organizations.

WHAT IS THE COVID-19 PANDEMIC TEACHING GOVERNMENTS ABOUT THE NEED TO MANAGE RISK?

All risk management professionals build programs and execute against them to address risk across the enterprise — whether from a pandemic, a cyberattack or another emergency. COVID-19 provided a reality check. It has shown us whether our initiatives are effective and aligned with the business. For some organizations, COVID-19 may have revealed a disconnect between how security and business leaders think about risk. A survey of more than 800 business and security leaders conducted by Forrester Consulting on behalf of Tenable shows that, as of mid-April, four in 10 organizations had experienced at least one business-impacting cyberattack due to COVID-related phishing. Yet, three-quarters of respondents said their COVID-19 response strategies were only somewhat aligned, at best.

YOU'VE SAID CYBERSECURITY IS UNIQUE BECAUSE IT'S A STANDALONE RISK AND A COMPONENT OF ALL OTHER ASPECTS OF ENTERPRISE RISK. CAN YOU GIVE AN EXAMPLE?

Common areas of concern for enterprise risk managers include strategic, reputational, operational, financial, legal and regulatory, and human resources. Let's consider strategic risk — which is the chance that some obstacle will keep an organization from pursuing its objectives. In a democracy, one crucial objective is to conduct free and fair elections. Any activity that could compromise the integrity of an election poses a serious risk. And possible risks include malicious cyber activity, such as hacking into voting systems to disrupt operations or change results. Cybersecurity professionals would play a key role in averting that kind of threat.

WHAT ROLE SHOULD CYBERSECURITY LEADERS PLAY IN THE BROADER FIELD OF ENTERPRISE RISK MANAGEMENT?

We cybersecurity professionals already provide risk management in our own realm. Risk management processes in other areas are similar to the ones we use, making it easy to apply our knowledge and experience to enterprisewide initiatives focused on strategy, operations, finance and other areas. If an organization isn't big enough to dedicate someone to risk management on a broader scale, it makes sense for the cyber professional to heavily influence or even own that function.

HOW DO YOU DEVELOP AN ENTERPRISE RISK MANAGEMENT PLAN?

It starts with interviewing senior leaders to help you define your organization's most critical functions, processes and services, plus the assets and systems it relies on to support those activities. Then, you need to determine what hazards could prevent your organization from providing the value or services it offers, and how likely is each of those hazards to occur. You can refer to industry surveys that highlight the risks to consider and the likelihood and potential impact of each one. The list you develop will include more risks than you can tackle, so the next step is to prioritize, working with your leadership to reach consensus on which risks are most important. That process leads to conversations about how to allocate resources — getting funds and people, implementing technologies, etc. Finally, as you implement the plan, you track those allocations quarterly.

Unfortunately, these conversations aren't happening at many organizations today. The Forrester study says only 40 percent of infosec leaders surveyed regularly review security performance metrics with their business counterparts. And just half work with business stakeholders to align cost, performance and risk reduction objectives with business needs.