Securing Security Funding: Qualitative and Quantitative Approaches

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "Securing Security Funding: Qualitative and Quantitative Approaches," on October 22, 2020. Accenture Security subject-matter experts, peer CISOs and board members examined how leading security executives are making the case for cybersecurity funding.

CISOs face new questions in funding cyber operations and innovations. How have budget decisions been impacted by the COVID-19 disruption, an increase in ransomware attacks and a more complex threat landscape? Is the cybersecurity budgeting process changing? What, if any, benchmarks, frameworks or tools are particularly relevant? What best practices should CISOs consider in gaining approval for new investments?

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

A volatile threat landscape threatens traditional budgeting practices

Securing funding for cybersecurity is a top CISO priority but rarely easy. As a CISO said, "Defining and justifying security is challenging. I need funding to run security and funding to build future security. But unless there's been a recent breach or the regulators are poking around, the process seems like a bit of a black box."

One CISO described budgeting on an annual basis, using a consistent budgeting framework that includes analysis of the threat landscape and measuring enterprise resiliency in terms of vulnerability and potential consequences. The CISO also leads a six-month review of the cyber budget with a wide collection of stakeholders and third-party advisors to validate priorities and investment levels. That discussion helps identify gaps and ultimately an action plan with additional investments, initiatives and actions.

A CISO said his budget framework focuses on four priorities: identify, detect, respond and recover, aligning to the NIST cybersecurity framework.

However, with the increasing volatility of the threat landscape, traditional annual budgeting processes can be inadequate. It is also becoming more difficult to calibrate the rate at which

actions should be taken, even when funding is available. The COVID-19 disruption is just one example of the kinds of intra-year volatility that are undermining traditional budgeting models. As one CISO said, “Threat actors don’t fit into our budget cycles.” Another CISO added, “The rate of change in the threat landscape is so rapid it doesn’t fit our financial models.”

CISOs think more agile approaches are required to address the inevitable but unanticipated threats. For example, a cybersecurity budget reserve, similar to a bad debt reserve, can provide the CISO with the flexibility and agility to respond to unexpected threats. One CISO said, “Management is starting to accept this as a result of all the incidents we’re seeing.”

Qualitative factors in securing funding

Qualitative factors under the CISO’s control are critical to success in the budgeting process. Successful CISOs start by building trust with business leaders, executive management and the Board. CISOs offered the following best practices for getting budget buy-in:

1. First build alignment of cybersecurity mission, vision and values. A CISO who had to drive transformational organizational change started the process by getting others to agree on a clear set of objectives: “protect, strengthen and enable.” From there, the CISO was able to get buy-in on specific foundational investments and initiatives.
2. Use simple measures/metrics to demonstrate value in terms that the Board and non-technical audiences can appreciate. Point back to objectives agreed to earlier and the capabilities you are trying to build and tie them to business enablement value.
3. Clearly explain the risk of gaps in cybersecurity defenses in business terms. Match business KPIs with key risk indicators to explain the value at risk without adequate cyber investment.
4. If budget discussions begin in the fall, deliver on the strategy and demonstrate value in the summer to create an environment conducive to productive conversations.

Quantitative factors in securing funding

It is also important to balance the case for funding with solid quantitative data about business outcomes. CISOs offered the following suggestions:

1. Explain the outcomes that investments will enable and their measurable value in business terms.
2. Avoid budget comparisons with other functions inside the enterprise. As a CISO said, “You’re competing against the bad guys, not other departments, enterprises or industry peers. We should be tracking investments to the threat landscape.”
3. Benchmarking is seen by some as inadequate, particularly since it doesn’t focus on outcomes and since every enterprise is at a unique level of cybersecurity maturity.
4. Look for application redundancies across the architecture. Sunsetting old applications may create more value than investing to strengthen their defenses.

5. Have business units/functions accept the responsibility of funding security investments that enable their capabilities. A CISO described this approach as more transparent since it requires clarity about investment levels, outcomes and value.
6. Treat cyber funding like insurance, enlisting actuaries to analyze the probability and impact of risk and calculate funding reserves.
7. One CISO said budget conversations should be linked to the enterprise crown jewels conversation—"How much money will we lose each day when operations are completely down as the result of a breach?"

Best practices for presenting to the Board

Talking at a high level with the Board, some of whom will not have deep technology or cybersecurity knowledge, requires a thoughtful set of quantitative and qualitative approaches. For example, a CISO discussed "The Wall Street Journal test," which Illustrates the reputation and material risks at play if an incident were covered on page one of the paper.

A Board member offered other advice:

1. Consistently use a framework such as a simple 2x2 matrix or other risk register templates. "Get the Board comfortable with why certain items are in the red zone and a clear description of the inherent situational risk," said a Board member
2. Focus on outcomes and results, not tools and technology. Match enterprise KPIs with key risk indicators
3. Put budget requests within the context of the business, its needs and risks. It also helps to put investments in the context of a journey—"Where we are, where we're going, how we're going to get there, and why it's important," said the Board member.
4. Deliver pre-read materials to the Board well in advance of their meeting so they have time to absorb the materials and prepare relevant questions.
5. Enlist the support of a Board member "sherpa" who will provide coaching before meetings and support during discussions.

Conclusion

Threat actors are starting to drive changes in the ways CISOs budget for cybersecurity. Traditional investment models, either relative to other departments or peer benchmarking, are proving inadequate for an increasingly dynamic threat landscape. An agile reserve of funding for unplanned incidents and unknown threats is emerging as a sound business practice.

Making changes to secure funding requires building trust with other executives and taking a balanced risk management approach that considers the needs and constraints of the business. It takes aligning cyber risk with business performance in ways that are unique and relevant for every organization. And most importantly, it requires consistently delivering value in terms the rest of the business understands and appreciates.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 509,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.