Assessing and Managing IT Security Risks

HIGHLIGHTS FROM THE WISEGATE SURVEY

About the Survey

Wisegate collaborated with Scale Venture Partners to conduct a member-driven, member-developed research initiative to gauge what meaningful IT security risks are growing, as well as which (if any) are shrinking. We wanted to understand what senior IT professionals identify as top risks, how confident they are in existing controls, and how they're measuring the significance of these risks. We gathered data using a hybrid approach: first by personally meeting with leading CISOs across 15 industries. Then, we expanded this study to a larger audience, conducting an online survey among a large cross-section of senior IT professionals to get a broader perspective and stronger conviction on the trends observed in the in-person conversations. Here are the results!

FINDINGS:

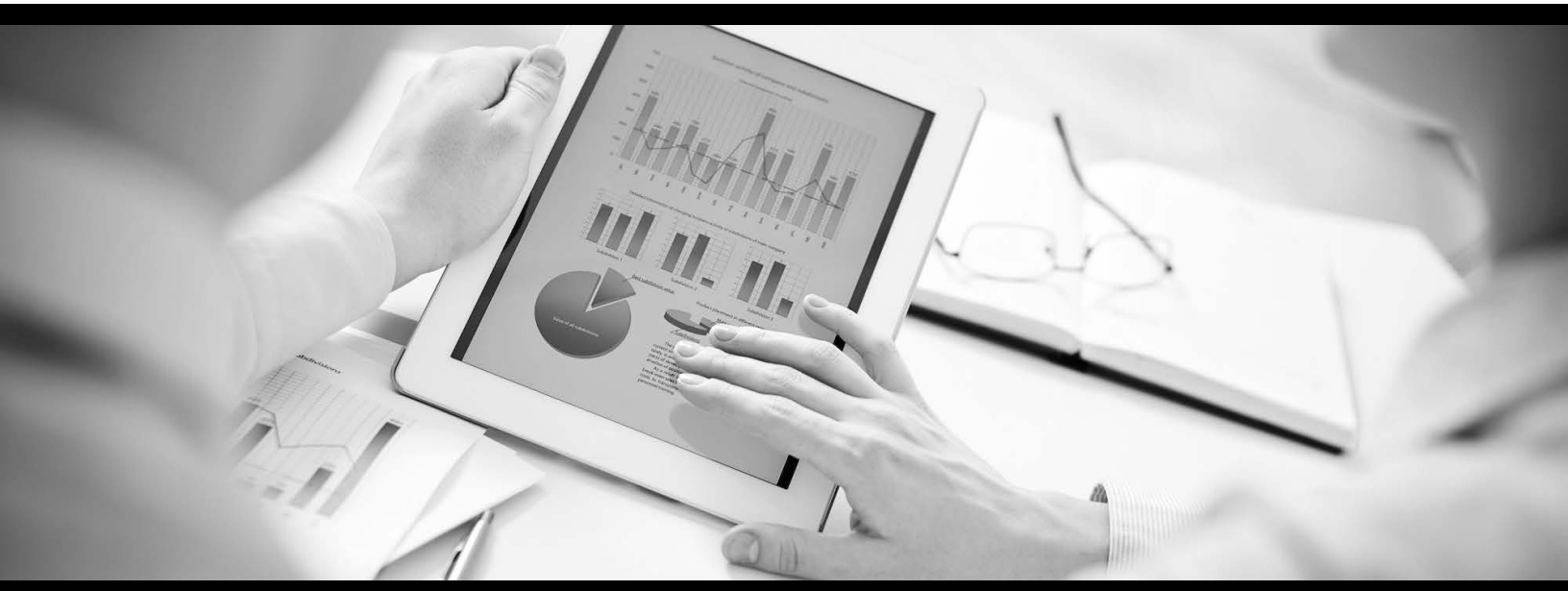
Enterprise Security Is Data Driven

Taking a data-driven approach is one of the most common strategies our respondents use for controlling enterprise risk and managing security controls. IT professionals hope to address enterprise security concerns more strategically by focusing on the data that needs to be protected, and applying these types of controls at every enforcement point.

Nearly half of respondents believe that information protection and control (DLP, tracking, masking, encryption) will be a top priority to their company in the next 3-5 years

IT organizations are losing control over the devices their end users want to use, the networks over which they communicate and the applications and infrastructure they use

IT pros hope to address enterprise security concerns more strategically by focusing on data.



FINDINGS:

How is IT Security Organized at Your Business?

In order to get a sense of the business context in which IT security professionals are working, this survey asked a few questions about the line of business to which the security function reports, how IT security is organized, and who is responsible for day-to-day security operations.

82% of security teams handle some or all of the operational security duties to secure their enterprise

Nearly half of IT security departments handle all of the IT-focused tasks, such as endpoint patching, antivirus updates and network firewall maintenance

54% of security teams rely on partners to implement security controls into their business operations

55% of security teams are aligned centrally as this enables the team to have tighter coordination and response times

37% of security teams are aligned with some blend of accountability

FINDINGS:

What are risks and trends driving your security programs?

With so many possible ways for harm to affect a company and its data, how do information security programs prioritize what to focus on, what threats to address first, and when to change their focus?

1. 2x as many teams use a risk-based approach over evaluating changes to their business strategy when prioritizing security risks

2. Security organizations are not prioritizing their program's maturity

3. Nearly three-quarters are primarily focused on the operational excellence of their own security efforts, raising concerns about building up security technical debt

4. A third of security teams (32%) plan 2-3 years out when creating and reviewing their strategic road map

5. There is often little security teams can do to predict long-term shifts in external threats

A third of security teams plan two to three years ahead when reviewing their strategic road map.

The consumerization of IT is one of the top three areas of current security concerns.

TOP THREE AREAS OF SECURITY CONCERNS

- Cloud technologies (both IaaS and SaaS)
- The consumerization of IT technology and services
- The proliferation of mobile devices, such as smart phones and tablets

TOP 3 SECURITY THREATS:

- Malware outbreak
- Breach of sensitive information
- Malicious outsider threat

Are security teams using automated, integrated security controls?

SECURITY TEAMS FREQUENTLY TRACK THREE AREAS OF GROWTH:

Enterprise size and complexity

Changes in the capabilities of adversaries looking to harm their company

Relevant regulatory compliance mandates

A LOOK AT HOW IT PROFESSIONALS ARE MANAGING THE INCREASED ENTERPRISE COMPLEXITY AND DEALING WITH INTEROPERABILITY AND MANAGEABILITY OF TECHNICAL SECURITY CONTROLS:

- 1/3 of security teams are making DevOps security controls a top priority
- 1/2 of respondents are using proactive threat/misuse detection or automated orchestration as a way to streamline their incident response plans and limit exposure windows
- 31% plan to participate in threat intelligence feeds and sharing platforms
- Nearly 12 consider risk-based authentication / authorization a top-three IAM security controls priority

The Bottom Line

IT is giving up control over most devices and infrastructure. This has profound implications to risk models and the types of controls that are effective going forward. In exchange, security programs are moving their controls closer to the business data and applications, and enlightened security teams are focusing on data-centric controls such as encryption and DLP to build scalable security solutions that meet the unique needs of their enterprise.

As concerns of security and compliance rise, teams struggle to map their security programs' efforts to business impact. In order to be competitive against increasingly sophisticated adversaries, security teams must look for ways to streamline their operational capabilities and provide actionable insights from an ever-growing set of security event data.

Read The Full Report

To read the full report, please visit http://www.wisegateit.com/library/assessing-managing-security-risks/.