ISSUE 7

Securely Speaking:

Your Privacy & Security Bulletin

BY **REBOOT COMMUNICATIONS LTD.**
WITH FOUNDING SPONSOR **GOSECURE**

1. **Smarter Security Budgets:**
   Lessons from Risk-Aware Industries
2. **Zero-Trust Adoption Across Government**
3. **The Synergy of Enterprise Security Risk Management and Organizational Resilience:**
   A Unified Approach to Security Leadership

Reboot COMMUNICATIONS LTD

info@rebootcommunications.com

GoSecure

WWW.REBOOTCOMMUNICATIONS.COM

Forward

Welcome to ***Securely Speaking: Your Privacy & Security Bulletin***, a regular quarterly publication provided by Reboot Communications Ltd. The bulletin's objective is to explore the latest trends and developments in privacy and security, including the challenges and opportunities that arise from new technologies like artificial intelligence, the Internet of Things, and blockchain. We also examine the legal and ethical implications of data collection and use, and look at how organizations and individuals can take steps to protect themselves and their information.

We invite you to review articles and interviews which will provide our readers with a comprehensive understanding of the complex and evolving landscape of privacy and security, as well as actionable advice and best practices for navigating it.

We believe that a better understanding of these issues is crucial for all individuals, organizations, and governments, and that by fostering a dialogue around privacy and security, we can work together to create a safe, more secure, and more ethical future for all. We hope you enjoy reading this bulletin and join us in this important conversation.

We focus on these strategic pillars to provide a comprehensive and valuable resource for staying informed and protected in the digital age:

OUR KEY STRATEGIC PILLARS

Education & Awareness/ Best Practices

Educating readers on the latest privacy and security threats, best practices, and emerging trends.

Thought Leadership & Industry News

Articles and interviews with experts in the privacy and security field.

Emerging Technologies

Emerging technologies and their potential impact on privacy & security (ie AI, IoT, blockchain).

Regulatory Developments

Information on the latest privacy and security regulations and laws.

Case Studies

Real world examples of privacy and security breaches and how they were addressed.

Acknowledgements

ARTICLE 01

Smarter Security Budgets: ***Lessons from Risk-Aware Industries***

By: Julien Turcot | Senior Vice President of Sales, GoSecure

ARTICLE 02

Zero-Trust Adoption Across Government

By: Jim Richberg | Head of Cyber Policy and Global Field CISO, Fortinet

ARTICLE 03

The Synergy of Enterprise Security Risk Management and Organizational Resilience: ***A Unified Approach to Security Leadership***

By: Tim McCreight | CEO and Founder, TaleCraft Security

ARTICLE 1

Smarter Security Budgets:
Lessons from Risk-Aware Industries


Image by standret on Freepik

Across industries, security has long been viewed as a necessary expense, but budgeting for it often feels more like guesswork than strategy. Established sectors like aviation and energy have set the standard for risk-based budgeting, allocating funds based on clear, measurable risks to ensure operations remain secure and disruptions are manageable. Yet, this disciplined approach to resource allocation has not been widely adopted, leaving many organizations exposed to unnecessary vulnerabilities or inefficiencies.

The cybersecurity challenge is no different: how can organizations ensure their investments align with actual risks, rather than reactive spending that may or may not address the real issues? A significant portion of budgets are often driven by regulatory requirements rather than proactive risk-based decisions. While compliance is necessary, it can lead to expenditures that do not always address the most pressing threats. The answer lies in adopting smarter budgeting principles informed by risk management practices already proven in other fields – prioritizing investments that mitigate real, high-impact risks while meeting regulatory obligations more efficiently.

When organizations take a structured approach to assess their current capabilities and gaps, they gain a clearer understanding of how best to allocate resources and prioritize investments. Without this foundation, even the most well-intentioned security strategies risk falling short.

How Established Industries Handle Risk

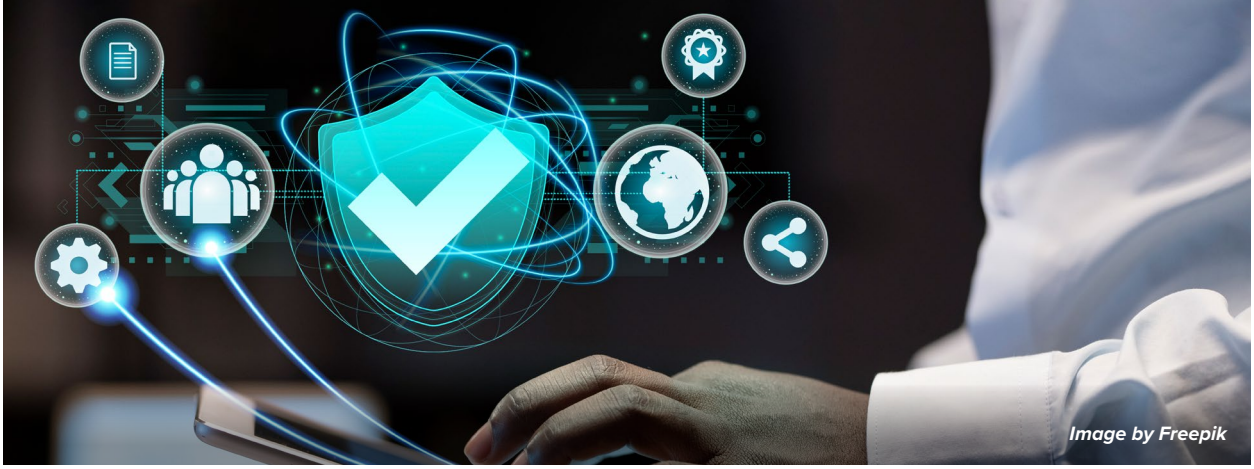
In sectors like aviation or power generation, risk assessments form the backbone of operational planning. Consider a power plant: if the risk of a shutdown is calculated to cost $10 million, it may decide to invest $50,000 annually in preventative measures. The goal is not to eliminate all risks, it's to balance the cost of mitigation against the potential impact, ensuring that critical functions remain stable.

This risk-aware approach enables these industries to allocate resources efficiently, focusing on areas that truly matter without overextending their budgets. This is a practice that ensures resilience and operational continuity.

The Gap in Budgeting Practices

Despite these clear advantages, this methodical approach has not been universally applied, especially when it comes to security. Across the board, many organizations are still developing their approach to aligning budgets with the scale and impact of potential risks.

Security budgets are often fragmented, driven by immediate concerns rather than a strategic understanding of potential threats. This fragmentation occurs because



various departments, such as IT, consume portions of the budget for initiatives like cloud infrastructure, OS hardening, and endpoint management, often without a unified security framework. Additionally, investments in areas like compliance audits, vulnerability assessments, and third-party integrations can further dilute focus. This approach can lead to overspending on low-priority areas while leaving critical vulnerabilities underfunded, ultimately creating gaps in an organization's overall defense strategy. A holistic, risk-informed approach is essential to maximize the impact of cybersecurity investments and ensure that spending aligns with real, high-impact risks.

A Smarter Path Forward

Adopting risk-based budgeting practices is not just a financial exercise, it is a strategic shift that can transform how organizations approach security. By quantifying potential threats and their impacts, decision-makers gain the insights needed to align spending with priorities.

An essential part of this shift is starting with a structured assessment that identifies where an organization currently stands in its security journey. This provides the baseline for effective resource allocation, ensuring that investments address not only immediate threats but also long-term strategic goals.

At GoSecure, we have seen firsthand how organizations can benefit from tools, such as Security Maturity Assessments, designed to simplify this process. By integrating risk analysis into the budgeting process, organizations can allocate resources more effectively, ensuring that their investments directly address the most pressing concerns. This approach also enables scalability, allowing companies to grow their security programs without unnecessary waste or guesswork.

The key takeaway: smarter budgeting does not mean spending more. It means spending wisely, ensuring that every dollar contributes to reducing risk in a meaningful way.

As industries continue to grapple with increasingly complex challenges, the importance of strategic security budgeting cannot be overstated. The goal is not perfection but progress, allocating resources in ways that make risks manageable and operations secure.

The lessons from established industries are clear: informed budgeting leads to better outcomes. By adopting a risk-based approach, organizations can transition from reactive spending to strategic investment, achieving greater efficiency and resilience.

Investing in a robust cybersecurity plan does more than just protect an organization, it builds trust, which is a powerful business enabler. When companies demonstrate a strong commitment to security, they reassure clients, partners, and stakeholders that their data and transactions are safe. This trust fosters stronger relationships, attracts new business, and opens doors to partnerships that might otherwise be hesitant due to security concerns. A secure organization becomes a more desirable collaborator, creating a competitive advantage in the marketplace. By strategically allocating budgets to enhance cybersecurity, businesses not only reduce risk but also position themselves as trusted leaders in their industry, driving growth and long-term success.

Security budgets should not feel like a gamble. With the right tools and methodologies, they can become a cornerstone of stability, empowering organizations to address risks effectively and confidently move toward their goals.

By: Julien Turcot | Senior Vice President of Sales, GoSecure | in www.linkedin.com/in/julienturcot

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry.

VICTORIA INTERNATIONAL PRIVACY & SECURITY SUMMIT

Strategies for Public Sector Transformation in the New World of Artificial Intelligence

Prepare to embark on a transformative journey as **Reboot Communications Ltd.** hosts the **Victoria International Privacy & Security Summit**. This groundbreaking 3-day summit will have over 750 delegates gathering at the Victoria Conference Centre in Victoria, BC on **March 11 - 13, 2025**.

This event will provide essential education, training and opportunities for ***CPD credits*** for individuals who are responsible for the transformation of the public and private sector into the new digital economy. The theme this year is ***Strategies for Public Sector Transformation in the New World of Artificial Intelligence***.

With the rapid rise of artificial intelligence (AI) and its transformative impact across various industries, safeguarding privacy and fortifying security have become paramount concerns. This international summit serves as a platform to address these challenges, exchange insights, and explore cutting-edge solutions to navigate the ever-evolving AI frontier.

Through dynamic multidisciplinary discussions, cutting-edge presentations, and interactive workshops, we aim to chart a course that ensures the benefits of AI unfold harmoniously with robust safeguards, redefining the landscape of privacy and security for generations to come.

VIPSS

WHY SHOULD YOU ATTEND THIS SUMMIT?

Here are a few compelling reasons:

1. Pre-summit educational workshops on March 11th.
2. Collaborate with senior executives who are changing the privacy and security industry.
3. Signature keynotes and concurrent keynotes by international subject matter experts in privacy and security.
4. Connect with like-minded companies, potential clients and industry influencers.
5. Unparalleled in-person networking via 1:1 meetings and small group conversations.
6. More than 30 exhibitor booths from our top tier sponsors.
7. Continuing Professional Development credits.

Your presence is not just an opportunity; it's a commitment to shaping a secure and private future for generations to come. Join us at the summit, where knowledge meets action, and privacy meets security!

Register Now and Save 15%!

Use the promo code **securely15** when registering to save 15% off the current rates!

REGISTER NOW

REGISTER NOW

Reboot COMMUNICATIONS LTD

WWW.VIPSS.CA

Reboot COMMUNICATIONS LTD

ARTICLE 2

Zero-Trust Adoption Across Government

Image by jannoon028 on Freepik

At local and federal agencies, the complex technology environment and the shift to remote work accelerated the adoption of zero-trust principles, emphasizing the need for secure and efficient operations outside traditional office networks. While the government had been aware of the various risks to the integrity of the software supply chain for many years, the massive SolarWinds compromise in late 2020 was a wake-up call. A remote access trojan attributed to a nation-state advanced persistent threat actor infected source code in a popular IT management product and compromised government networks and private sector companies, including critical infrastructure providers.

At many agencies, people started looking at zero-trust architectural philosophies more seriously, realizing that the traditional "castle and moat" approach of keeping malicious actors out and implicitly trusting everyone inside the network perimeter was a fallacy.

With zero-trust security, trust must be established each time there's a connection and ideally revalidated as new applications are opened and even as new types of activity are undertaken. Zero-trust is based on identity and access management. This concept is coupled with least privilege access, which is a cyber equivalent of the "need to know" principle that the national security has operated under for many years. For example, if a user or device only needs to read data to accomplish the task at hand, don't bestow the authorization to write a file or to delete it.

Image by rawpixel.com on Freepik

Remote Work Becomes a Reality

Remote work also posed challenges for network architecture and for application performance. Some agencies require that remote users' access to cloud-based applications be routed back through the agency's data center rather than a nearby cloud point of presence. This latency increased cost and degraded user experience, introducing performance problems to latency-sensitive applications such as online-meeting software.

Even though users could get their work done, the situation was not ideal. Over time, it became clear that users needed an environment that worked seamlessly so they could work successfully and share data safely and securely with partners no matter where they were located. The combination of zero-trust with IT technologies such as software-defined networking (SD-WAN) and cloud services makes it possible for users, devices, compute resources, and data to seamlessly connect regardless of where any of those four elements may be located.

Image by pressfoto on Freepik

The Power of Partnership

After I retired from government, I used to have spirited and almost theological debates with former peers in government who said that zero-trust could not be done at scale or not for their particular use case. But one of the things I learned when I left government and went to work in the private sector was that technology companies already had solutions that effectively addressed most of the elements of zero-trust and that some companies and government entities had effectively implemented zero-trust approaches across complex global operations.

The good news is that implementing better security, especially regarding zero-trust, is a partnership. Government does a good job of creating conceptual frameworks and vendor-agnostic technical reference architecture and strategies. However, implementing zero-trust even within government agencies is almost exclusively done using commercial off-the-shelf products.

More good news is that many midsized companies and virtually all large corporations are implementing zero-trust, so agencies don't have to reinvent the wheel. Because they can leverage the power and diversity of solutions being developed for the private sector market, agencies are likely to find solutions that fit their price point, mission needs, and technology stack.

Unfortunately, the news isn't all good. Many organizations struggle with technology integration across vendors, which underscores the need for broader industrywide collaboration. Although many vendors are adding security capabilities, the solutions are often siloed, particularly regarding the policy enforcement points crucial to implementing zero-trust at speed and scale.

It's important to realize that implementing zero-trust doesn't happen in isolation. There is nontechnical work to be done, starting with getting leadership buy-in, including finding an active executive champion and educating the workforce. Helping the average user understand how zero-trust can help them become more productive and even provide a safety net against the consequences of an innocent mistake are important first steps.

When it comes to technical implementation, an agency's starting point should be determined by its technology roadmap. Working on identity and agency management is a good first step, but if you're already refreshing a different part of your technology infrastructure that happens to align with some other aspect of zero-trust, such as policy enforcement, that should be your starting point instead. While the destination for zero-trust implementation is the same for all, each agency will proceed at a different pace and along a different path to get there.

By: Jim Richberg | Head of Cyber Policy and Global Field CISO, Fortinet
jrichberg@fortinet.com | www.linkedin.com/in/jim-richberg

Jim Richberg's role as Fortinet's *Head of Cyber Policy* and Global Field CISO at Fortinet leverages his 35 years' experience leading and driving innovation in cybersecurity, threat intelligence, and cyber strategy.

For over 25 years, Fortinet has been a driving force in the evolution of cybersecurity, including the convergence of networking and security. Learn more at **www.fortinet.com**.

ARTICLE 3

The Synergy of Enterprise Security Risk Management and Organizational Resilience: A Unified Approach to Security Leadership

Image by Freepik

In today's complex threat landscape, security leaders must shift from a reactive stance to a proactive, strategic approach. Enterprise Security Risk Management (ESRM) and Organizational Resilience (OR) are two interwoven disciplines that, when properly aligned, create a robust, forward-thinking enterprise security program that not only protects assets but also ensures long-term business continuity and adaptability.

ESRM: The Foundation of Proactive Security

ESRM is a risk-based methodology that integrates security into business operations by aligning security strategies with organizational objectives. It prioritizes risks based on business impact, ensuring security programs support the company's goals rather than operating in a silo. This approach enables security leaders to move beyond compliance-driven checklists and instead focus on risk mitigation strategies that are directly tied to business success.

As I have often stated in my presentations, "Security is a business function, not just a technical or operational issue. If we fail to align security with business goals, we fail to provide real value to the organization." This perspective underscores the necessity of embedding ESRM principles into decision-making processes at all levels.

Organizational Resilience: Strength in Adaptability

Organizational Resilience takes ESRM principles further by ensuring that businesses are not just protected from threats but can also recover and thrive in the face of disruption. OR encompasses business continuity, crisis management, and adaptive risk management, helping organizations withstand incidents ranging from cyberattacks to natural disasters.

By integrating resilience into security strategies, businesses can prepare for the unknown, minimize downtime, and maintain stakeholder confidence. As I often discuss in TaleCraft Security workshops, "True resilience isn't just about bouncing back; it's about bouncing forward with lessons learned, emerging stronger and more prepared for future challenges."

The Power of Integration: A Security Program That Endures

The real value of ESRM and OR lies in their integration. When combined, they create an enterprise security program that not only identifies and mitigates risks but also ensures business continuity and operational flexibility. This approach allows security leaders to:

- Anticipate risks more effectively by leveraging ESRM's proactive risk assessment.
- Enhance business continuity planning by embedding resilience strategies into security functions.
- Foster a risk-aware culture that empowers employees to understand their role in maintaining security and resilience.
- Strengthen stakeholder trust by demonstrating a commitment to not just protecting but sustaining the organization.

As I shared during a recent TaleCraft Security seminar, "Security leadership today is about more than just responding to threats – it's about preparing for the inevitable and ensuring your organization can continue to operate under any circumstances."

Practical Steps for Security Leaders

Security professionals looking to align ESRM and OR should consider the following steps:

- Conduct a Business Impact Analysis (BIA) to understand critical functions and their dependencies.
- Develop an integrated risk framework that incorporates both security threats and business resilience factors.
- Engage with senior leadership to ensure security initiatives support business objectives.
- Foster cross-functional collaboration between security, IT, HR, Operations and other business units.
- Continuously assess and evolve the program to address emerging threats and organizational changes.

Conclusion

The future of security leadership lies in the convergence of ESRM and Organizational Resilience. By adopting this unified approach, organizations can create a security program that not only defends against threats but also ensures long-term success and stability.

Security is no longer just about protection – it's about resilience, adaptability, and strategic alignment. By embracing ESRM and OR as complementary forces, security leaders can help their organizations not just survive but thrive in an unpredictable world.

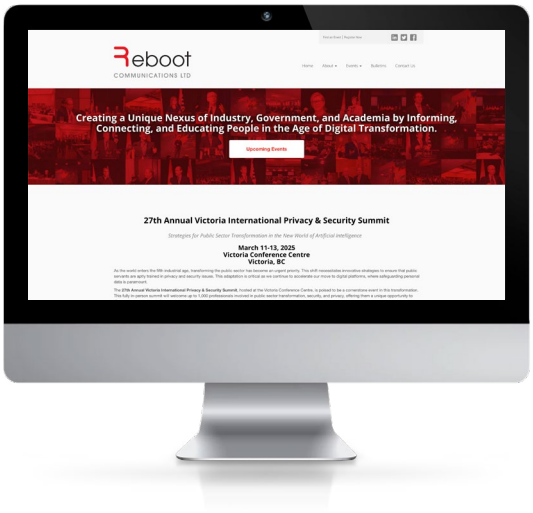
By: Tim McCreight | CEO and Founder, TaleCraft Security
tim.mccreight@talecraftsecurity.com | www.linkedin.com/in/tim-mccreight-a0bb204

For more insights on ESRM, Organizational Resilience, and security leadership, connect with Tim McCreight and TaleCraft Security at **www.talecraftsecurity.com**.

Copyright

ISSUE 7 EBOOK EDITION | *FEBRUARY, 2025*

Editor: **Greg Spievak**



FIND OUT MORE & SUBSCRIBE

For more information or to subscribe and receive the ***Securely Speaking: Your Privacy & Security Bulletin*** regularly, email info@rebootcommunications.com.