GUIDE

Secure C-Suite Buy-In for an Information Security Platform

Your Guide to Creating an Effective Proposal

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

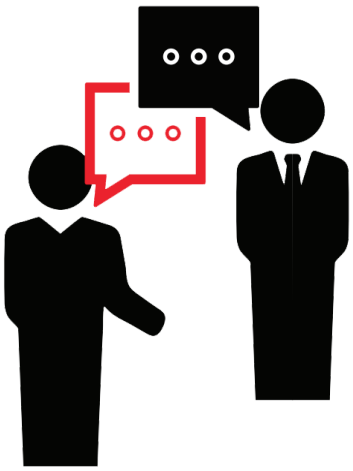
Introduction

If you have ever been involved in selecting a software solution for your organization, you know that it can be a significant financial investment. The process typically requires extensive research and, most likely, approval from the highest levels of management – not just the CTO or CIO, but the CFO, CEO, and/or other C-level leaders as well. As a member of the information security (infosec) team, you are already well-versed in the need for effective vulnerability risk management (VRM) and the value that the right VRM solution has in keeping your organization secure by facilitating the prioritization and remediation of vulnerabilities. However, obtaining the budget for an infosec platform investment may require you to bring management up to speed on that value first. This guide can help you to present an effective and compelling case to the C-Suite (or its equivalent in your organization) in order to obtain their buy-in and approval for investing in the right VRM platform.

Start By Putting Yourself in Their Shoes

Before you start to dig into the details of researching solutions and putting together your proposal, pause to consider the people to whom you will be presenting. Of course, this will differ in every organization depending on its structure and decision-making processes. (In some companies, the leaders' equivalent to the C-Suite may have titles that do not begin with "chief," such as "owner" or "president." For the purposes of this guide, we are referring to any of the leaders in your company whose approval is required to make the investment.) Regardless of their roles or titles, there are two main things to consider up front: their level of IT competency and your readiness to put your case into business terms.

You Are the IT Translator



Depending on your business, often, the people you must convince to commit resources and money to an IT solution will not have a strong IT background themselves. Most of their days are taken up with the business of their subject area, such as finance or marketing, or, in the case of the CEO, the overall vision and strategy guiding all areas of the business. They likely do not have time to learn about the intricacies of a technical solution, or they may have a cursory functional technical knowledge at best.

As the IT expert, you will naturally have done extensive research on the technology's features, functions, and requirements for

configuration and integration in your existing IT environment. Whether they acknowledge it or not, senior level leaders rely on the IT team to understand the technical details of the infosec platform, and they will be looking to you to help them translate those into business terms and connect the solution's benefits to business outcomes.

Prepare to use data to connect your infosec needs and the IT platform's functions with the business outcomes your managers are trying to achieve. The most important thing you want the C-Suite to take away is how the VRM solution will protect and/or benefit your organization strategically and financially. You know that a good IT program does not exist solely to benefit the IT team; it benefits the whole organization. Gear your presentation toward demonstrating how the VRM solution you recommend will make business sense not just for you, but for your leaders - making their jobs easier, or helping them to be more effective.

The most important thing you want the C-Suite to take away is how the VRM solution will protect and/or benefit your organization strategically and financially.

Prepare to explain, qualitatively and quantitatively, the return on investment (ROI) the C-Suite can expect to see by implementing the VRM platform you recommend. For example:

Risk Reduction: This is the most obvious and likely strongest case for your VRM investment. What are the risks that your organization incurs by not implementing the security platform? How would the financial investment and implementation costs of your solution compared to what it would cost to recover if your organization suffered a security breach that could have been prevented had you had the right solution in place? (For more on

risk reduction, see the section below on Information Security by Industry.)

Compliance: Especially in highly regulated industries (like healthcare or financial services), compliance goes right along with risk reduction as a top business reason to invest in a solid VRM solution. How does the investment compared to the costs of being fined, paying legal fees, or having your reputation damaged because of a HIPAA violation or a penalty due to non-compliance with PCI or NYDFS regulations?

Efficiency and Cost Reduction: The VRM solution you choose should be focused on prioritization and remediation of vulnerabilities – reducing the time that the IT team spends on manual work while smoothing out security workflow, communication, and reporting processes. Ultimately, these benefits should lead to quantifiable reduced costs (such as through less overtime pay for IT employees) and a more efficient work environment that can be framed in terms of ROI for the C-Suite.

Mission and Strategy Impact: For for-profit and nonprofit organizations alike, a more qualitative argument can be made about the effects that a security breach would have on your organization's core purpose and strategy. For instance, maybe you work for a healthcare organization with a mission of caring for patients. Achieving your mission relies on maintaining their trust, and your goal is to mitigate the risk of patient data theft. Be ready to articulate what it would mean to your mission if such a

breach occurred that damaged patient trust, and how this weighs out against the time and money that implementing a security solution would require.

Profit and Financial Sustainability: If you work in a for-profit organization, profit is ultimately what your C-level leaders have in mind. Consider what effects those potential breaches, compliance costs, efficiency drains, and mission interruptions have on profit margins down the line. If you do not work for a for-profit entity, address how the budgets and financial sustainability of your organization as a whole could be affected by choosing or not choosing to implement the proposed VRM solution.

When talking numbers, don't forget that the financial investment in your VRM solution does not only include the price tag of the software. It also includes the cost of staff time to implement it and the opportunity cost of committing team resources to the project that would otherwise be spent on other company priorities.

Information Security by Industry

The business case for good cybersecurity is strong in any industry. Here, we list some of the most commonly attacked industries along with security trends in each that you can use to formulate the basis of your business case.

- **Financial Services:** Financial data will always be a top target for hackers for obvious reasons. Even large and powerful institutions are not impervious to threats; months later, experts are still piecing together the extent of the damage caused by high-profile breaches on major financial institutions like the one that affected the SWIFT global bank messaging system in 2015[1]. A recent survey[2] of worldwide financial institutions found that their greatest infosec challenges included:
    - Fast-evolving and sophisticated technologies
    - Assessing and monitoring security of third-party vendors
    - Customers' growing use of mobile devices for banking and payments
    - Threats from outside of the institutions' home countries

- **Healthcare:** If you work in healthcare, you are already aware of HIPAA and the need to be compliant. However, being HIPAA-compliant does not necessarily mean your organization is secure, and organizations must learn how to think beyond compliance. Healthcare is seeing one of the highest and fastest-growing rates of cyberattacks, especially due to trends such as:
    - The high value of medical identity theft to hackers coupled with the growing volume of electronic protected health information (ePHI)
    - Historically lax security by healthcare institutions

[1] "Banks urged to tighten security as hacks continue." CNN Money. August 31, 2016. http://money.cnn.com/2016/08/31/technology/swift-bank-hacks

[2] PwC. "Turnaround and transformation in cybersecurity: Financial services." Accessed September 2016. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/industry/financial-services.html

    - Human error, a top source of security breaches in any organization, but compounded by high-stress, high-speed environments common to healthcare

- **Software-as-a-Service (Saas):** SaaS vendors' customers place an enormous amount of trust in them to deliver their services securely and continuously. The main security challenges of your customers' industries become your main challenges as well. Others unique to the SaaS business may include:
    - Keeping up with industry standards to which your customers are subject (such as HIPAA for healthcare customers or PCI for financial institutions)
    - Ensuring security while maintaining round-the-clock uptime that customers expect
    - Performing sufficiently frequent backups and encryption of customer data
    - Minimizing the introduction of vulnerabilities into new software releases while keeping up with market expectations for your product's functionality
    - Maintaining data segregation

- **Government:** Government organizations at all levels have a big job protecting themselves from hackers, hostile foreign governments, and terrorists who seek to disrupt operations and obtain valuable sensitive data. Just ask the U.S. federal government's Office of Personnel Management, which estimated in 2015 that over 20 million personnel records may have been compromised by a high-profile attack by a foreign entity involving social engineering, a third-party contractor,

and malware[3]. Critical challenges for government organizations include:

- Assessing and monitoring security of private contractors
- Addressing weaknesses of legacy IT systems
- Assuring continuity of security operations in the case of a major disaster
- Maintaining sufficient security resources and infrastructure in the face of public budget pressures

- **Energy:** PwC's 2016 Global State of Information Security survey found that the oil and gas industry reported more cybersecurity incidents in 2015 than did any other industry surveyed[4]. As with other types of businesses, quickly-evolving threats, security awareness training for staff, and monitoring security among third-party vendors are top concerns. In addition, the energy industry's unique challenges include:
  - The appeal to hackers and terrorists as a target based on political reasons and/or the energy industry's criticality to every other sector of the economy and governments
  - A need for energy companies to retrofit older electronic infrastructure with updated protections
  - The nascent nature of technological solutions available to protect operational technology (OT), even as OT it is increasingly interconnected with IT environments

[3] "Hacking of Government Computers Exposed 21.5 Million People." New York Times. July 9, 2015. https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html

[4] PwC. "Turnaround and transformation in cybersecurity: Oil and gas." Accessed September 2016. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/industry/oil-gas.html

Preparing Your Case

Now that you have put yourself in the mindset of the C-Suite, you are ready to begin researching VRM solutions. A good practice is to narrow your list to the top three solutions that you believe are the best fit for your organization's needs. You are not just investing in a product, but in a relationship with the VRM vendor as well, so gather as much information as you can about these things:

- **Company:** Your primary goal in researching the company is to understand their experience level, trustworthiness, and cultural fit with your organization.
    - **Chief Technology Officer:** Research their background in VRM as well as their experience working in or for your industry.
    - **Company Reputation:** Look for testimonials and case studies, especially from companies in your industry or, if not in your industry, ones that have similar risk profiles and business models to yours.
    - **Support:** Be confident that the vendor's support team is going to be responsive and effective if you have issues. Will you just be a number in a ticketing system, or will you be considered a valuable client? This is another area where a testimonial or reference from one of their existing customers can be valuable. Make sure that the vendor's hours of operation are sufficient, and ask them what their typical response and issue resolution times are. You might even consider making

a test call to the support line to see how quickly you reach a live person.

- **Location:** Although it is common to work with vendors who are not located in the same city or region, find out if the vendor has to travel to provide service or if being in a different time zone could affect your ease of communication with them.
- **Solution:** For a more in-depth look at how to thoroughly evaluate a VRM solution, see our white paper, “Improving Business Outcomes with Vulnerability Risk Management.” Narrow your list to the top three solutions based on:
- **Features and Benefits:** Schedule a demonstration with each vendor so you can see these firsthand. Allow enough time to ask detailed questions about how the platform works and the ways that these features translate to furthering the goals you are addressing in your business case.
- **Pricing:** At this early stage, the vendor will probably provide a price range that will depend on multiple factors. Understand what this range will be and the factors it depends on.
- **Implementation Timeline and Resources:** Ask the vendor what a typical implementation schedule looks like, and how this will affect internal resources.

An Example of How to Translate Your Business Case

Tech Talk	C-Suite Delivery	Business Driver
"Our prioritization process is manual. We know we can streamline the process if we acquire a prioritization tool."	"Two members of our IT Team have been manually prioritizing our vulnerability risks and takes an average of one week to finish the process. By getting the proposed software solution, we can reduce remediation time to hours, and reallocate the manpower to other important projects.	• Utilize talent with more urgent duties within them team • Improve employee engagement • Utilize company resources efficiently

Bringing It All Together: Making Your Presentation

Depending on the structure and culture of your organization, you may present your business case in the form of a written proposal, a formal presentation, or participation in an informal discussion. Time limits and the presentation format may mean that you do not explicitly present or share all of the information below. However, be prepared to speak to all of the following in case the C-Suite asks. But be concise – like you, your audience is time-crunched. In addition, it can be powerful to find a manager (if you are an individual contributor) or a peer (if you are a manager) to advocate for your recommendations as well. Brief them on your analysis and get their input on the business case in order to present the strongest recommendation.

- **Benefits and Weaknesses:** Outline the benefits of each solution in comparison to the other options being considered, as well as each one's strengths and weaknesses as they relate to your business goals and challenges.
- **Expected ROI:** Present your analysis of the return on investment based on each solution's required investments and the business outcomes – risk reduction, improved compliance, better efficiency, mission achievement, and higher (or protected) profits – that you expect it to deliver. • Implementation Risks: Even the best solutions come with risks. The best thing you can do is be aware of and prepared for them.
- **Implementation Costs:** Include the software's price tag as well as additional costs like extra staff time needed for implementation. • Implementation Timeline: Indicate how quickly the VRM solution will be up and running. • Expected Implementation Resources: Estimate how many staff and how much of their time will be required. • Your Recommendation: Recommend the solution that you think is the best fit for your company based on your research and analysis.
- **Implementation Timeline:** Indicate how quickly the VRM solution will be up and running.
- **Expected Implementation Resources:** Estimate how many staff and how much of their time will be required.
- **Your Recommendation:** Recommend the solution that you think is the best fit for your company based on your research and analysis.

Having a C-Suite mentality is key to getting buy-in for investing in the right VRM platform. There is a strong business case for every organization to invest in a good information security program and the tools you need to make it successful. Secure your leaders' buy-in by developing your business case and using data to demonstrate how the right VRM solution will achieve the business outcomes your management seeks.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.