Developing a more powerful risk report for your board: spotlight on financial services
The risk climate facing financial services board of directors

Board members at financial services institutions (FSIs) are under a tremendous amount of pressure, particularly when it comes to managing risk. They're well aware that it's not just data they're charged with protecting. It's their customers' money, personal financial information and most importantly their trust.

In this industry, the costs of getting it wrong are extraordinarily high. Pressure comes from all sides: financial services ranks as one of the least-trusted industries, and also one of the most targeted by cybercriminals. New cybersecurity disclosure requirements and changing legislation like GDPR compounds the situation.

No board member wants to preside over a massive reputational crisis or see the company end up in the hot seat at government hearings. Even smaller-scale issues can result in massive customer churn in a world where customers have more options and easier mobility than ever before.

At the same time, the risk climate in financial services is changing rapidly. According to the consulting firm BDO, almost all (97%) financial services companies say they're embarking on a digital transformation. These transformations often include new technology investments in things like cloud, IoT, AI, customer experience and more. All these new changes bring new risks to the forefront.

To fulfill their oversight duties in this high-stakes situation, board members need FSIs to provide reliable and actionable risk reports. In this eBook, we detail how risk and security professionals working in financial services companies can better serve their board members.
Common challenges in presenting risk to FSI boards

Cybersecurity and risk are on the agenda of every quarterly board of directors’ meeting. Successful board presentations on risk offer an efficient, effective and realistic look at the risks to the business. However, achieving that outcome is not always easy. Security and risk professionals face major challenges, including:

• **Achieving the Right Level of Detail:** Board members often bring industry expertise or come from a wide variety of backgrounds. They may not have deep experience in the world of cybersecurity, digital governance or risk. If you don’t prepare for this, you may end up providing either too much or too little detail to enable an effective conversation.

• **Ensuring Data Integrity:** Disparate systems and “sources of truth” can also be a major problem. Within any financial services enterprise there may be multiple business units using a wide variety of risk and security tools. Without a centralized method for producing accurate data, you may end up producing different lists of issues with different rating systems. This hurts credibility and makes it hard for the board to gain a clear and holistic sense of the risk environment.

• **Achieving Presentation Consistency:** Manual one-off methods for reporting risk enable cherry-picking. Some reports to the board may be designed to carry a specific message or advocate for a certain budget request, instead of providing a data-driven look at the most critical issues facing the company.
Five ways to improve your board presentations on risk

1. **Build credibility.** Board members need to know they can trust the risk reporting coming from within the financial services enterprise. Part of this comes from having the appropriate credentials, but even more can be built through authentic communication.

FSI board members don’t need reports that understate the seriousness of issues facing the business. They don’t need to hear an exhaustive report of all the good work the risk function is doing. Instead, build trust by sharing a candid account of business risks and where existing efforts fall short. Also, since the threat climate in financial services changes rapidly, ensure you’re communicating when new risks arise.

2. **Establish a common language and be consistent in using it.** It’s critical to establish a common framework to use in reporting to the board on risk, security and compliance. Ideally, this should be something you can repeat over and over again, with standard nomenclature and easy tracking of key performance indicators and ongoing issues. Yes, your reporting should be flexible enough to adapt to emerging issues, which is much easier if you already have built a solid foundation.

This could include a standard dashboard that provides an at-a-glance look at the issues facing the business. Color-coding items red, yellow and green might seem like an oversimplification, but it provides an easy way for the board to grasp the information. As long as the data that drives the color-coding is reliable and consistent, this method provides a clear, digestible and consistent picture.
3. **Focus on the most critical items.** Board meetings tend to have a lengthy agenda, and risk is only one part. What board members really need to know are the most critical security issues facing the business and the plan to resolve them. The choice of which topics to cover should come directly from an informed assessment of the risks facing the company.

Once the topics are clear, determine what level of detail the board needs to provide informed oversight.

4. **Commit to a data-driven approach.** You shouldn't need a separate process and data analysis approach to report to your board. Instead, your reporting approach should be a direct output from your risk management approach, and both should be driven by real-time data analysis. A good cybersecurity methodology is based on a solid foundation, one single source of truth from all risk management tools. Ideally, a version of that same dashboard can become the basis for your presentation to the board.

5. **Seek feedback.** Your board of directors can be a valuable source of input. Their experience means they may be seeing trends and risks outside of your domain. Your presentation isn’t just a report-out, it’s a chance for you to learn what they’re seeing within other businesses, what they’re worried about and gain input into your approach.

---

**How much security is enough security?**

Given the emphasis on risk in financial services around the world, it’s likely that at some point in reporting to the board, you’ll be asked if cybersecurity and risk management is efficiently funded.

It’s not always an easy question to answer. Risk professionals are aware, like all other professionals, of competing financial priorities and the importance of producing return on any investment.

In these situations, it’s important to ask yourself what the appropriate level of threat defense is in your situation.

We recommend a simple test. Imagine you’re in a disaster scenario. Could you stand in front of your board and customers and say that you did everything possible to avoid this scenario? In the financial services industry, what you’re protecting is vital – and your approach should reflect the seriousness of that charge.

---

**How much security is enough security?**

Given the emphasis on risk in financial services around the world, it’s likely that at some point in reporting to the board, you’ll be asked if cybersecurity and risk management is efficiently funded.

It’s not always an easy question to answer. Risk professionals are aware, like all other professionals, of competing financial priorities and the importance of producing return on any investment.

In these situations, it’s important to ask yourself what the appropriate level of threat defense is in your situation.

We recommend a simple test. Imagine you’re in a disaster scenario. Could you stand in front of your board and customers and say that you did everything possible to avoid this scenario? In the financial services industry, what you’re protecting is vital – and your approach should reflect the seriousness of that charge.
Conclusion: Building a solid foundation for risk reporting in financial services

Establishing an effective reporting relationship with the board is mission critical in the effort to combat financial crime. These are vital stakeholders – charged with protecting the company, its investors and customers. Like risk and security professionals, they are committed to protecting the company from security threats.

As FSIs continue their digital transformation, they will need to invest in new technologies that meet customer expectations and empower new services. However, technological innovation has also opened a world of new opportunities for cybercriminals, and financial services companies are one of their top targets.

By arming board members with the right information, security and risk professionals can ensure that digital transformation in financial services does not come at the cost of risk mitigation.

At ServiceNow, we believe effective board presentations start on a solid foundation of data. We designed our governance, risk and compliance products to give businesses a single source of truth to monitor and prioritize risk. And, on that solid foundation, they can build a relationship with their board that ensures their company appropriately prioritizes risk in the future.
The future of the financial services industry is dependent on balancing innovation with risk mitigation. At ServiceNow, we’re committed to giving cybersecurity professionals the tools they need in this climate.

Learn More About our Governance, Risk and Compliance Solutions

Learn More About How ServiceNow Works for Financial Services