servicenow

Now on Now: How the Now Platform® enables effective cybersecurity and risk presentations to the board of directors

Table of contents

Cybersecurity and risk are on the agenda of quarterly board of directors' meetings for every public company. Contextualized briefings and productive discussions are essential for fulfilling the board's oversight responsibilities and managing cyber risk. Given the complexity of these issues, the potential impact, and the time constraints of regular board meetings, IT, Security, Risk, and Audit leaders often struggle with presenting their findings to boards in a succinct yet impactful way.

At ServiceNow, our Security Operations and Risk products have helped us manage risk to our business and our customers. Because they are fully integrated with other ServiceNow products on the Now Platform®, we can better manage our overall cybersecurity program. We have visibility into how we are managing multiple forms of risk, and what we are doing to address vulnerabilities. In addition, they have helped us prepare reports and provide updates to ServiceNow leadership—including the board of directors—that paint a clear picture of our risk landscape and enable them to make effective decisions.

Common challenges

IT, Audit and Security teams face multiple challenges when preparing for discussions with the board:

- **Data integrity** – Data often resides in multiple systems and multiple formats and must therefore be consolidated and reconciled. Any discrepancies in the data can stall the discussion, create confusion, and delay important decisions.
- **Data gathering** – Collecting and rationalizing data manually from multiple sources is a very time-consuming, resource-intensive process that, because of the human factor, can introduce errors or gaps in the data.
- **Level of detail** – Given the varying depth of knowledge that CIOs, CISOs, and board members bring to the table, it's challenging to find the right altitude for the presentation, i.e., to provide a level of detail that is meaningful for substantive discussions while avoiding data overload and jargon that can sometimes cloud rather than illuminate the issues.
- **Presentation consistency** – Critical to building credibility with the board quarter-over-quarter is a common framework and language for presenting data. This is difficult to do when building custom reports using information from multiple sources.

Keys to success

Here are some of the lessons we've gained as we've used the Now Platform and matured our program:

- **Consistent reporting mechanisms** – Adopt the same platform and familiar presentation for board reports that your organization uses to measure its performance. This not only simplifies data gathering and formatting, but also makes preparation easier, because we are already familiar with the data. Answering questions promptly and thoroughly builds credibility, and trust.
- **Unified approach to monitoring risk** – Monitoring the health of the organization using a common platform like the Now Platform establishes a consistent process, improves data reliability, and eliminates the need to integrate data from disparate systems.
- **Common control framework** – Use a control framework that is widely known, such as NIST (National Institute of Standards and Technology) or CIS Top 20 (www.cisecurity.org/controls/). The common controls can be used to achieve compliance with myriad regulations, while simplifying how you rate your performance against them. The Now Platform provides this capability and enables risk from different environments or systems to be represented in a uniform way. This facilitates executive-level discussions about risk in all areas of the business.
- **Balanced detail** – Work with the board in advance to determine the appropriate level of detail needed for the board to provide informed oversight. For us, this means explaining the company's current risk level and trends and evaluating the overall risk management program against industry best practices.
- **Key trends, programs, and investments** – Ensure that one of your consistent reports shows trending for key metrics/KPIs on a quarter-over-quarter basis, with adequate detail to demonstrate that programs are driving down risk. Risk and cybersecurity are dynamic—a company can be in good shape one day and in trouble the next—so be sure to show how investments and resources are prioritized based on risk, and how risk changes from quarter to quarter. We use ServiceNow Project Portfolio Management for cybersecurity reporting because it shows the correlation between risks and programs.
- **Transparency and focus** – Be completely candid with the board about any changes in the company's risk profile. New cyberthreats are a constant. Risks can also arise from internal process changes, new vendors, and technical innovations introduced by digital transformation. Therefore, it's essential to demonstrate that the program can handle new risks over time. Also, focus the board on the most critical risks to the organization to demonstrate where you are prioritizing precious resources. Seek their feedback on what they believe are top focus areas.
- **Automation** – Continually improve the impact of your cybersecurity and risk programs by embracing automation—for example, embedding risk and compliance into digital processes to enable continuous monitoring of risk, or automating the security runbook and the patch management process. Automation also helps improve consistency, efficiency, accuracy, and productivity, while driving down cost. At ServiceNow we've seen a 2.5X efficiency gain through automation for security incident response alone. Automating routine tasks also frees up security staff to work on more interesting activities, which improves their job satisfaction and helps us retain top talent.

Case Study: Cybersecurity risk management

We use our own products to gather data from other platforms, tools, and data sources and consolidate it in the Now Platform, so that it's native to any workflow. We can draw on that data and apply our experience to create reports that demonstrate our risk and compliance posture both internally and on our customers' instances. We have implemented more than 350 security controls (leveraging the NIST framework), which are compiled in the ServiceNow Governance, Risk, and Compliance (GRC) portfolio of applications that we use to manage risk and remediation efforts. These controls are mapped along two dimensions: importance (an assessment of both likelihood and impact) and strength (an assessment of how mature our control implementation is). They are rolled up into a heat map, which is color-coded red, yellow, and green. This makes it easy to highlight the areas that need attention or discussion. There's no need to reconcile data from multiple sources, and we have clarity on our most critical risks that require board attention.

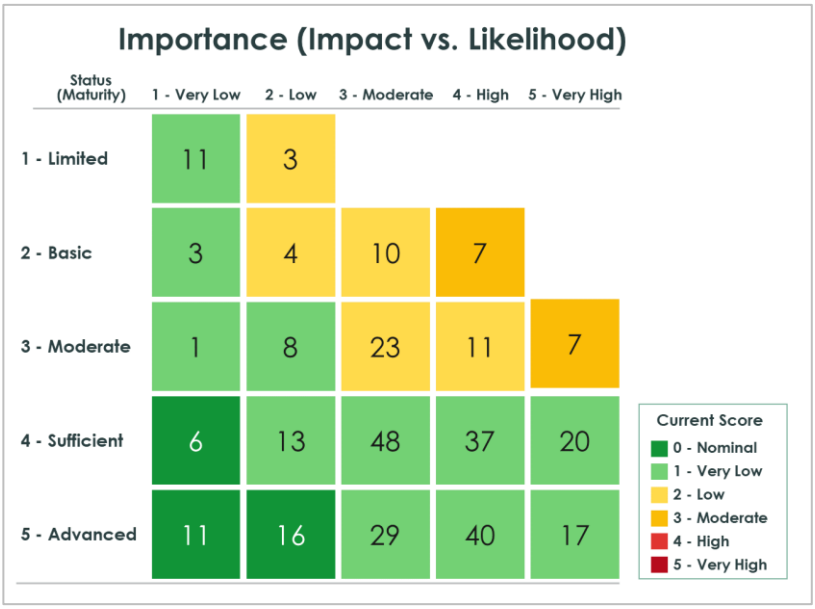

Figure 1 This heat map illustrates risk in terms of likelihood and impact. The numbers show the number of controls for each area.

When controls fail and risk exposure is created, we use the CMDB to prioritize risk, and use cross-functional workflows to assign issues, remediation tasks, and communicate risk to other departments. By having this centralized within GRC, board reporting on current issues, risk exposure, and delays is straightforward with no additional steps. Time is spent resolving issues rather than figuring out how to report them to stakeholders.

Case Study: Cybersecurity incident response

Another report example is incident response, which reports on metrics like Time-to-Identify and Time-to-Remediate that are tracked by the ServiceNow Security Operations product. As in the above example, we can easily extract metrics and insert them into the report. We also can slice data in multiple ways, such as showing trends over time.

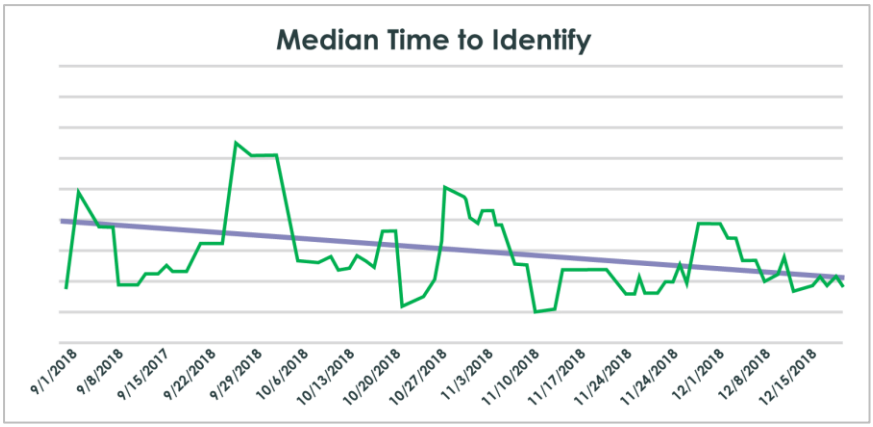

Figure 2 This graph shows the time to identify a threat each day in a quarter. The board can see that the median time to identify is shrinking.

Boards recognize that resolving security vulnerabilities is a critical part of protecting the company's infrastructure and keeping services running that deliver revenue and customer satisfaction. For this we use ServiceNow Vulnerability Response, which connects security and IT teams, provides real-time visibility, and automates cross-functional workflows, helping us respond faster and more efficiently to vulnerabilities. By measuring our program against KPIs, it lets us show the board that we're meeting our SLAs, and that our processes are repeatable over time.

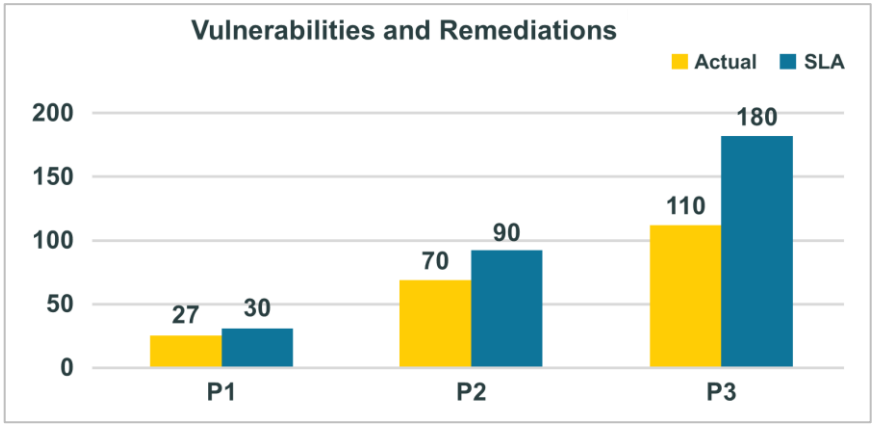

Figure 3 This chart compares the number of days to address vulnerabilities with our SLAs. The board can see that we are not only meeting but beating our SLAs.

These reports also help our discussions with our insurers, who are constantly evaluating our risk. Insurers want to know not only how likely we are to be attacked, but also how prepared we are to respond. We can show them that our incident response time has steadily decreased over time because we've implemented the right tools or capabilities. This increases their confidence in covering us.

About ServiceNow

ServiceNow is changing the way people work. We bring security, risk, and IT together on a single platform, enabling customers to quickly Identify and prioritize security incidents, vulnerabilities, and enterprise risks, and respond faster using workflows, automation, and orchestration.

Now on Now is about how we use our own ServiceNow solutions to work faster, smarter, and better. With Now on Now, we're achieving true end-to-end digital transformation. To learn more, go to www.servicenow.com/nowonnow.

For product information go to www.servicenow.com/grc or www.servicenow.com/sec-ops.