TANIUM

Reporting on risk in the public sector

Experts offer insights and guidance for reporting risks in today's highly distributed world.

TANIUM

Reporting on risk in the public sector

Experts offer insights and guidance for reporting risks in today's highly distributed world.

Contents

Expert advice on reporting risk

Managing risk is one of the top responsibilities of any leader in the public sector. But they can only manage the risks they know about. And with silos that often plague public sector agencies of all types, from the federal government to K-12 school districts, there can be many unknowns. Ensuring service continuity, as it turns out, starts with reporting on your agency's level of risk.

This eBook is about reporting risks to your organization's decision makers, so that stakeholders can make informed decisions about reducing risks - ensuring your ability to deliver services and protect valuable data.

If you're new to performing risk assessments, we recommend that you read our eBook on measuring risk to learn about interviewing subject matter experts and building risk probability calculations that go into risk reports.

In this eBook, our focus will be the reporting of risk. That means finding the right information to share with decision makers and sharing it so it can be acted on effectively.

At the end of this eBook, we'll present a checklist, summing up the advice.

Reporting risks that matter to agency leaders

Risk means a lot of things to a lot of different people. If you're in the IT department, you'll probably hear about the risk of server outages or data breaches or software vulnerabilities that could lead to data breaches.

You might also hear about unauthorized devices, bring-your-own-device (BYOD) policies, and how difficult it is to monitor what employees are doing with the organization's data on their home networks, if they're working remotely.

All those things — from server outages to remote employees — represent risks of one kind or another. But if you're in charge of reporting risk to your organization's leaders, do you really want to give them a list of unpatched assets or an estimate of how many employees or students are using BYOD devices?

What risks does your organization ultimately care about?

To answer that question, let's ask about risk itself. Fortunately, there's a generally agreed-upon definition of risk, at least among IT professionals. ISO 31000, the International Standards Organization's guidelines for risk management, defines risk as "the effect of uncertainty on objectives."

"Uncertainty" seems straightforward enough. If something is certain, there's no risk involved. If we know absolutely that our power systems have functional backups, there is no risk of power loss.

But what about "objectives?" Every employee, team, department, and organization has objectives. When reporting risk to department heads and elected officials, you need to ask yourself which objectives they care about. It's not that they're indifferent to the goals of individual teams and projects. But leadership's job is to focus on the big picture.

Here are three objectives you can be sure your organization's leaders care about:

- Data confidentiality, integrity, and availability
- Delivering services to constituents or students
- Regulatory compliance

There may be other objectives, such as protecting your reputation and the public's trust. But you can be sure that your agency leaders care about protecting important student, employee and constituent data, avoiding IT outages that bring constituent services to a halt, and ensuring that the organization never makes headlines about embarrassing ransomware.

Each of these objectives will likely require detailed reporting to support the overall risk assessment. For example, the data leadership cares about can include everything from constituent and employee data to student or medical records. All of these data types need to be managed and secured.

Different types of data may be facing different risks of varying severity. Agency leaders will need to know how much this objective is at risk overall, as well as what specific types of data might require new investments in security or personnel training.

Before you prepare a report about risk in your organization, make sure you understand your agency's objectives. Some of those objectives might be posted on your organization's website. But others might be listed in an internal, long-term strategic plan. One way or another, though, you need to know what those objectives are, because you're going to use them to frame your discussion of risk.

As we mentioned in our eBook about measuring risk, all the risks you should be tracking and reporting to agency leaders should relate in some concrete way to these high-level objectives.

For example, it should report on any risks to people, processes or tools that are essential for your organization's ability to stay open and deliver services. If a mission-critical data center is known to be behind on its patch schedule, that risk matters, not just because patching is a best practice, but because unpatched servers are more likely to succumb to security attacks or suffer from performance problems.

For more information about creating weighted measures for risk, see our eBook **The Power of Certainty: measuring endpoint risk in the public sector.**

Your risk report should provide the agency leaders with the information they need to make smart decisions about which actions to take to mitigate risks related to the organization's objectives.

If you're presenting risk information and your audience seems bored or mystified, it's probably because you haven't framed your discussion around the topics they care about.

CHAPTER 2

Identifying risks helps you think like an attacker

There's an added benefit to framing your risk reports this way When you've identified risks to your data and to the organization's ability to deliver constituent services, you've also identified the weak points that cyber criminals and hostile nation-states might attack.

After all, when a cybercriminal tries to break into your organization's IT systems, what are they doing? Most likely, they're either trying to get to your data to steal it or leak it, or they're trying to get to the systems that process your data and disrupt them, possibly through ransomware or some other form of attack.

Because you're now measuring and reporting risk based on strategic objectives, you have a detailed, weighted report on the weakness and vulnerabilities related to your data and the systems that store, process and present your data. You know what's most likely to be targeted and how to go about protecting it, based on your detailed knowledge of vulnerabilities, probabilities and so on.

All this supporting information makes the risk assessment you're presenting to leadership much more credible and useful. Agency leaders see how data and service continuity are at risk, what controls are in place to mitigate those risks, and how those controls could be improved or broadened to reduce risks further in keeping with the organization's overall goals.

CHAPTER 3

Risks involve IT operations, not just IT security

Being able to deliver constituent services, 24/7, means ensuring employees have everything they need from the IT group to stay productive and support the organization's initiatives. Ensuring service continuity requires assessing and mitigating risks to websites, databases, constituent or student portals, email servers, business processes, and more.

It also requires taking a step back to look at what new initiatives and tools your organization is planning to roll out for stakeholders and which of those initiatives might introduce new risks to the organization.

Finally, operational continuity might involve IT processes such as patch management, employee training both inside and outside the IT department, or among private-public partnerships.

Your organization's leadership needs to understand the risks involved in each of these areas, as well as the cumulative risks that affect the organization's ability continue to offer services without disruption.

CHAPTER 4

Share the report with the groups that helped you create it

In our eBook on measuring risk, we stressed the importance of talking to stakeholders in individual departments and units to learn about their perceptions of risk. They'll likely know about risks and priorities that you might miss just from scanning asset inventories in the IT department.

Now that you've generated a report, share your findings with these stakeholders. Get their thoughts on the ways risks have been measured and reported. And after leadership has had a chance to review the report, share any news about areas of opportunity for improvement, and so on with the report's contributors.

People want to know that they've been listened to and understood. By sharing the results of the report, you close the loop with people you talked to early in your risk management process, and you make it more likely that they'll contribute to risk assessments in the future.

CHAPTER 5

Put systems in place to accelerate reporting

In many organizations, reporting on risk is an annual or quarterly activity – if you're lucky. But risks are shifting all the time. Regulations change. New malware variants are created. And new digital transformations can shift priorities, eliminate some risks and create others.

Put IT systems and workflow processes in place to help automate and accelerate data collection for risk reporting. That gives you a much more timely and accurate report of risks at any given moment. It also makes it easier to quickly assess and respond to risks.

One important requirement for automating risk analysis is being sure you can collect real-time data from endpoints – desktops, laptops, tablets, smartphones, and servers your employees depend on. By gaining real-time access to what's happening on endpoints, you'll gain insights into employee productivity, threat status, IT resource utilization and more.

Risk reporting as an ongoing practice

With cyber threats increasing and the pace of attack on the public sector moving faster than ever before, it's vital for agency leaders and elected officials to understand and mitigate risks that could jeopardize their major initiatives. That understanding begins with effective risk reporting.

In this eBook, we've discussed what makes risk reporting successful. We've stressed the importance of understanding risk as uncertainty about objectives and aligning risk measurements with the objectives your organization cares most about.

We also talked about how focusing on these objectives can help your security team identify how cybercriminals might target your IT infrastructure.

Ideally, risk reporting should be an ongoing practice. Risks are continually changing, whether they're arising from new initiatives or new types of cyber threats. Automating data collection and risk assessment helps provide your organization's leadership team with the vital information they need for making the right decisions to mitigate risk and protect sensitive data, and ensure constituent services are offered at all times.

To learn how the Tanium platform helps public sector organizations track and manage risk across departments with one view, learn more about our Organizational Risk Scoring with **Tanium Benchmark**, visit **Tanium.com** or **request a demo today.**

Risk Management checklist

1. Meet with your organization's leaders to understand their long-term objectives.
2. Assign these objectives a score to understand the relative importance of each.
3. Identify the people, processes and technologies that support each objective.
4. Explore the uncertainties about each supporting factor in an objective's supply chain.
   - Whenever possible, rely on automation to collect data, such as data about the operating status of endpoints.
   - Meet with stakeholders in various departments to understand their concerns about risks and to collaborate on recommendations for reducing those risks.
5. Assign each uncertainty a score in terms of importance and a percentage in terms of likelihood. Multiply scores by the likelihood to derive a risk score for a particular person or team, process or technology in an objective's supply chain.
6. Tally the results of your measurements and organize them in a way that relates each risk to one of the main objectives.
7. Meet again with your department head for a data-driven discussion about risk. Help them understand existing risks and the decisions that can be made to reduce them.
8. Now that you have a risk measurement framework in place, continue updating it, using automation whenever possible so that risks can be assessed in detail at any time.
9. Use your risk reporting to guide your security planning. Now that you know where risks lie in the areas of data security and service continuity, take appropriate action to reduce those risks.