TANIUM

Expose the uncertainty:

Best practices for reporting risk

Experts offer insights and guidance for reporting risks in today's fast-moving, highly distributed environment.

TANIUM

Expose the uncertainty: Best practices for reporting risk

Experts offer insights and guidance for reporting risks in today's fast-moving, highly distributed environment

Contents

Expert advice on measuring risk

Managing risk is one of the top responsibilities of any leadership team seeking to achieve strategic objectives But leaders can manage only the risks they know about. Effective leadership, it turns out, depends on risk reporting, awareness and communication.

This eBook is about reporting risks to your company's executive team and board of directors, so they can make the right decisions about reducing risks and helping your company achieve its strategic objectives.

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 itself. That means finding the right information to share with your company's leadership team 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.

CHAPTER 1:

Reporting risks that matter to a company's leadership

Risk means a lot of things to a lot of different people. If you talk to IT people about risks, 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 company's data on their home networks now that 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 company's executive team and the board, do you really want to give them a list of unpatched systems or an estimate of how many employees are using BYOD devices?

What risks does your company's leadership team 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 servers will never crash, there's no risk of them crashing.

But what about "objectives?" Every employee, team, department, and business has objectives. When reporting risk to the executive team and the board, 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 the job of a company's leadership is to focus on the big picture.

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

- Data confidentiality, integrity and availability
- Business continuity
- Regulatory compliance

There may be other objectives, such as a certain percentage of revenue growth or a good reputation in the marketplace. But you can be sure that your company's leadership cares about managing and protecting its important data, avoiding IT outages that bring business to a halt, and ensuring that the company never makes headlines about regulatory fines.

Each of these objectives will likely require detailed reporting to support the objective's overall risk assessment. For example, the data the board cares about encompasses everything from customer data to employee data to financial records to intellectual capital such as product designs and patents. All those types of data need to be managed and secured.

Different types of data may be facing different types of risks of varying severity. The board 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 leadership team's objectives. Some of those objectives might be posted on your company'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.

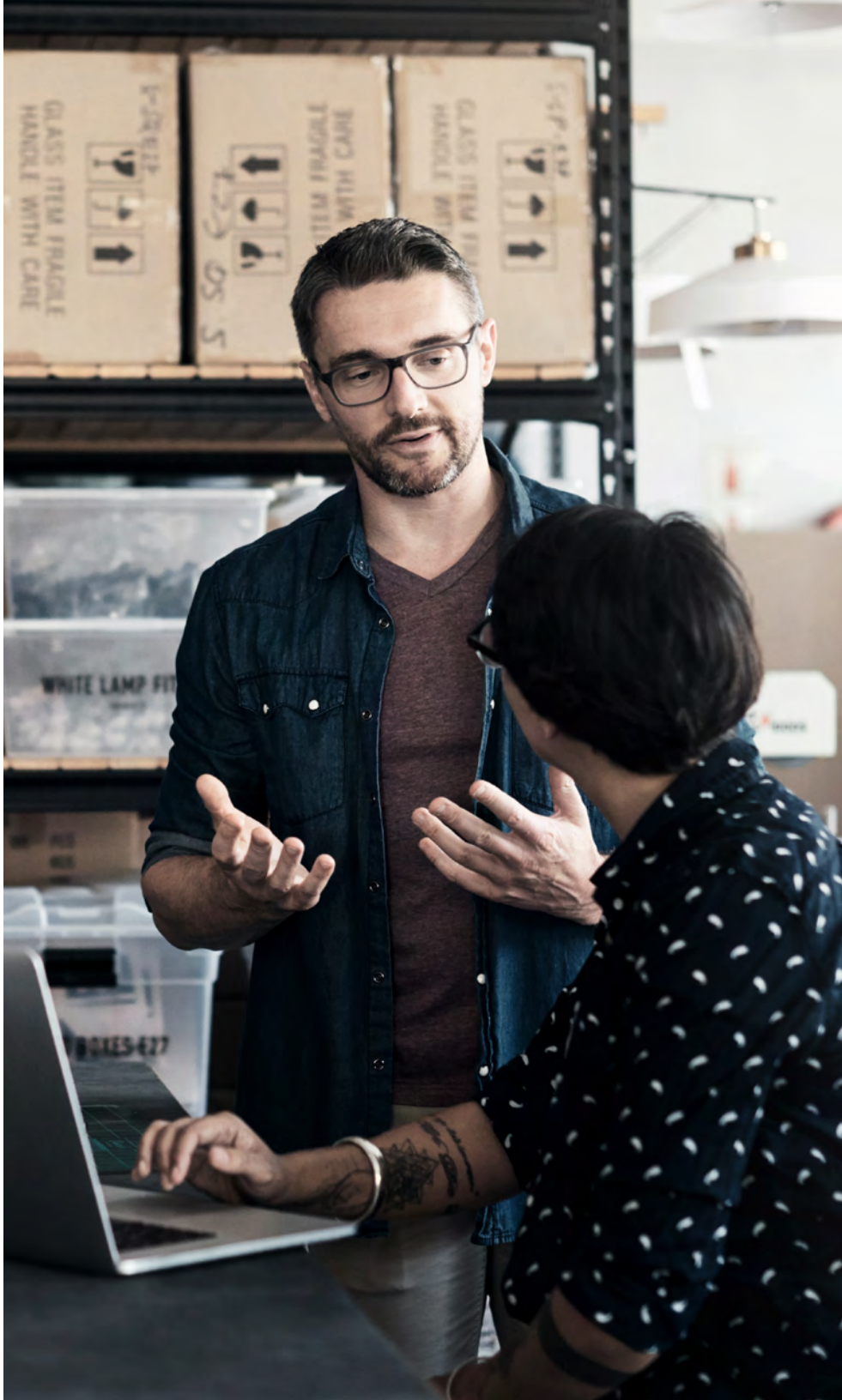
As we mentioned in our eBook about measuring risk, all the risks you should be tracking and reporting to the leadership team should relate in some concrete way to these high-level objectives.

For example, it should report on any risks to people, processes or technologies that are essential for your company's business continuity. If a business-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 *What You Don't Know Can Hurt You: Expert Advice on Measuring Risk.***

Your risk report should provide the leadership team with the information they need to make smart decisions about which actions to take to mitigate risks related to the company's strategic 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 the leadership team really cares 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 company's business continuity, you've also identified the weak points that criminal syndicates and hostile nation-states might attack.

After all, when a cybercriminal tries to break into your company'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, though, 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 them, based on your detailed knowledge of vulnerabilities, probabilities and so on.

All this supporting information makes the risk assessment you're presenting to the board much more credible and useful. The board sees how data and business 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 company's overall strategy.

CHAPTER 3:

Risks involve IT operations, not just IT security

Business continuity means ensuring that employees have everything they need from the IT organization to stay productive and support the company's partners and customers. Ensuring business continuity requires assessing and mitigating risks to websites, databases, financial systems, email servers, business processes, and more.

It also requires capacity planning, especially if the company is experiencing growth. And capacity planning, in turn, might lead to new cloud migration projects, new technology purchases, or the development of new applications, all of which might introduce new risks to the organization.

Finally, business continuity might involve IT processes such as patch management, employee training both inside and outside the IT department, and partner relationships.

Your company's leadership needs to understand the risks involved in each of these areas, as well as the cumulative risks that affect the company's ability to achieve its business continuity objectives overall.

CHAPTER 4:

Share the report with the business units that helped you create it

In our eBook on measuring risk, we stressed the importance of talking to stakeholders in individual departments and business 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 the leadership team and the board have had a chance to review the report, share any news about new investments, shifting priorities, 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. But risks are shifting all the time. Regulations change. New competitors enter markets. New malware variants are created. And new business initiatives and 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 risks when new threats arise or when your company takes on a new market or adopts new technology.

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 businesses moving faster than ever before, it's vital for business leaders to understand and mitigate risks that could jeopardize their business. 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 strategic objectives your company's leadership team cares most about.

We also talked about strategic objectives common to most organizations, and how focusing on these objectives can help your security team identify how cybercriminals might target your company's IT infrastructure.

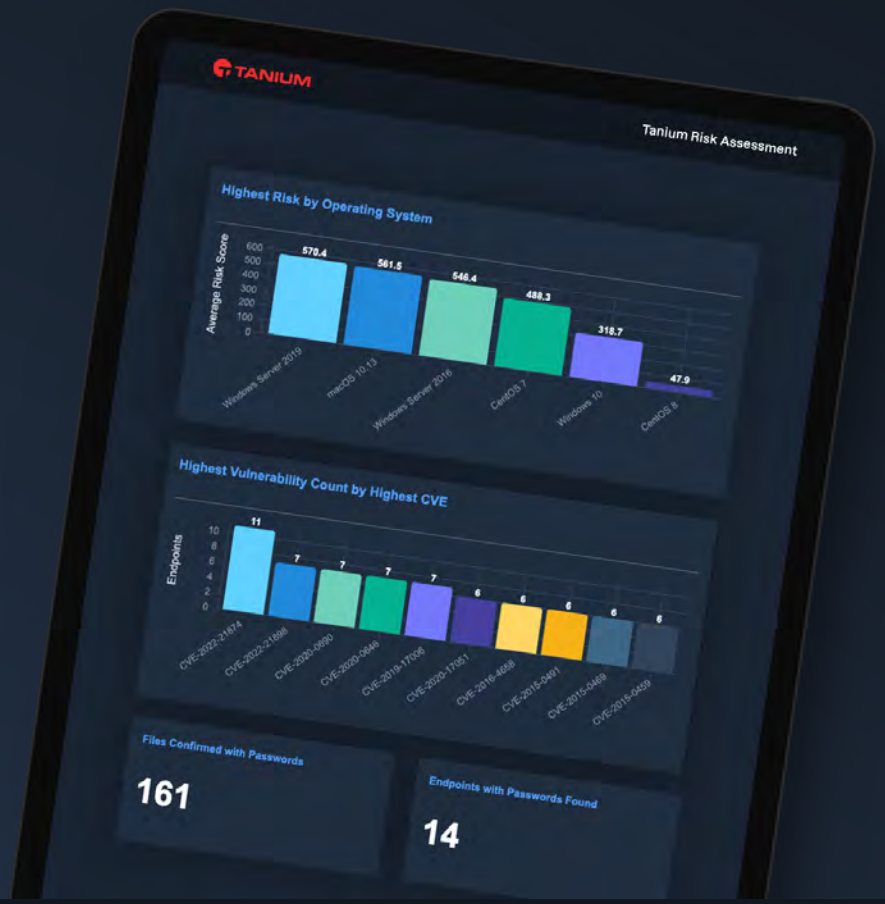
Ideally, risk reporting should be an ongoing practice. Risks are continually changing, whether they're arising from new business initiatives or new types of cyber threats. Automating data collection and risk assessment helps provide your company's leadership team with the vital information they need for making the right decisions to mitigate risk and advance the company's objectives.

Endpoint devices play an important role in risk assessment and reporting. The Tanium Converged Endpoint Management (XEM) platform can help give organizations more visibility into their security metrics, so they can identify risks and remediate them in real time. Tanium Benchmark is the only solution that provides real-time risk comparisons to industry peers.

Learn more about **Tanium Benchmark.**

Score your endpoints against multiple risk vectors and industry benchmarks — in 5 days at no cost.

Learn more →



Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.