




BRIGHTER

Chaos, order and risk:
how organizations can tackle
ransomware

Illuminating insight
from Countercept



Ransomware. As anyone working on the frontlines will tell you, it has been one of the most prevalent and pernicious threats over the past few years. It's highly visible – and often a hot topic for public debate – even accounting for the sampling bias inherent in our role as responders. It's hard to ignore the impact these incidents have on their victims – they're immediate, real, and damaging.

A successful ransomware attack can bring an organization to a standstill, making it unable to access critical data or systems that are vital for day-to-day operations. Only the theft of currency has a more direct impact to an organization's bottom line. But while currency theft is largely confined to a small group of organizations in the relevant industries, ransomware is universal: it does not care what industry you are in.

Data loss, while potentially more impactful to the reputation of an organization, tends to have a more delayed and dispersed financial impact. Regulatory fines often come several years after an incident, and the loss of business gets spread out over a longer period. This results in a less sharp economic shock for victims, and is not as immediately visible on an organization's balance sheet as a ransomware incident.

What is the risk of ransomware to your organization?

Assessing risk is probably one of the biggest dilemmas security leaders face, and how an organization tackles it can have significant impact. So, where to start? Impact is only part of the picture. To calculate the risk, you also at least need to factor in the **probability** of the threat.

How do you quantify probability?

It's the million-dollar question. Quantifying the probability is difficult and, as is well covered by our head of sales enablement, Paul Brucciani¹, humans are notoriously bad at estimating it. This is especially relevant to cyber security risks, as we tend to lowball the probability² of a negative event where the chance is greater than 30%.

There is no one-size-fits-all solution on how to calculate risk. If you ask ten senior decision-makers about the probability of their organization suffering a ransomware attack, you'll get ten different answers, using ten different methodologies. Those employed at relatively mature organizations may say the probability is low. Those who have suffered a breach recently may say it is likely – though notably employing some hefty recency

bias. Each of those questioned could be correct in their judgement, but equally they could all be entirely wrong. This may seem like a bold assertion, but it is one that rings true when you speak to many senior decision-makers in cyber security who have no clearly defined methodology for calculating risk. Considering that risk plays such a central role in cyber security, it is a major failing of our industry that there's no established best practice approach to calculating it – something we should work together to fix.

¹<https://www.linkedin.com/pulse/how-worlds-best-risk-decision-makers-decide-paul-brucciani/>

²<https://www.jstor.org/stable/1914185?seq=1>

Steps to self-improvement

First, it is important to acknowledge that there is no magical mathematical formula you can use to calculate risk, so you shouldn't try. Numbers are solid, they are defined, they give people confidence and a shared common language with business colleagues. But they can be dangerous and provide a false sense of confidence in an outcome purely because it has a numerical value assigned to it. The probability of ransomware impacting an organization is complex, with a wide range of variables at play and no reliable quantitative data to support such an approach.

In the wider risk-management field, there has been a move to using quantitative approaches, but this has been fueled by the availability of reliable statistical data. However, when this data wasn't available, traditional risk management tended to use more qualitative approaches. Cyber security is a field where the extraneous nature of many variables (e.g. the adversary) makes the accurate quantification of risk incredibly difficult.

Risk decisions need to be informed, but the decision-maker will never have perfect information to be able to assign solid numerical values to calculate risk. Ultimately, you will be making a judgement using imperfect information; therefore, you are assessing the risk rather than calculating the risk. This differentiation in terminology is important as it helps to frame the problem and ultimately what you are trying to achieve.

One field that can provide answers, however, is 'intelligence'. The intelligence field has been around for many years and has devoted significant time in to making assessments to answer difficult questions with imperfect information. Threat intelligence, the cyber cousin of intelligence, is much newer but heavily references traditional intelligence theory and methodologies.

Intelligence, or intelligence assessment, is not a perfect science and has suffered some largescale and particularly public failures, including the 1941 attack on Pearl Harbor and the 9/11 attacks in the US. Nevertheless – or perhaps because of this – the sector continues to develop processes and tools to make more effective assessments. In a primer authored by the US government, the key problems facing those in intelligence are identified:

“The perennial problems of intelligence: the complexity of international developments, incomplete and ambiguous information, and the inherent limitations of the human mind. Understanding the intentions and capabilities of adversaries and other foreign actors is challenging, especially when either or both are concealed.”³

Do these problems sound familiar to you? Complexity, incomplete information – particularly about unseen adversaries – and our own psychological limitations are problems facing cyber security risk decision-makers every day. However, all hope is not lost, as there are some key lessons to take away from the intelligence field that will help you better assess risk and make more informed security decisions.

The most powerful step is to acknowledge and be aware of cognitive bias, and then minimize these through sound analytical methodology. In intelligence parlance, this would be the use of structured analytic techniques, which in practice are a wide range of techniques³ that can help improve analysis.

These techniques can be broken down into three categories:

- **Diagnostic techniques** – help to ensure assumptions, analytic arguments and limitations are more transparent and therefore rigorous.
- **Contrarian techniques** – challenge assumptions and presumed wisdom of current thinking.
- **Imaginative thinking techniques** – help to develop new insights, perspective and analyze alternative outcomes.

³<https://www.e-education.psu.edu/sgam/sites/www.e-education.psu.edu/sgam/files/TradecraftPrimer-apr09.pdf>

Structured analytic techniques sound like a dusty academic term with no real-world application, but they are not. You will unconsciously employ many of these techniques every day in your personal and professional life. Key examples of useful techniques for conducting cyber security risk assessments are:

- **Key assumptions check** – this is a diagnostic technique that involves reviewing the key assumptions that judgements rely on. This is a challenging cognitive exercise but can be very valuable in ensuring that assessments are not based on inaccurate assumptions. In cyber security, this could have many applications and can commonly be seen in how decision-makers factor in threats and opportunities that may exist based on technological exposure.
- **Quality of information check** – this diagnostic technique is a key feature of any critical thinking and something we do unconsciously every day. For example, when crossing a road, we rarely rely on only our hearing to establish that it's safe to do so – bicycles and electric cars make very little sound. Most people look to verify there's nothing approaching, because they have more confidence in visual data in this situation to be sure they can cross safely.

Consciously checking the quality of information is useful for assigning confidence to assessments and helps identify gaps in collection that can be fixed in the future. Some information you have may be opinions, and weighting these can be difficult between multiple sources but is possible. This exercise can help seek out data points that may support one view or another.

- **High-impact, low-probability analysis** – this is a contrarian technique which aims to ensure that low-probability events are analyzed and considered in decision-making. The benefits of conducting this analysis include the discovery of a correlation between key factors that can enable decisions that influence both high- and low-probability events. A key example of such an event in cyber security would be the analysis of ransomware incidents.

- **Outside-in thinking** – this is an imaginative thinking technique that focuses on considering the external factors in the analysis process. This is especially beneficial in cyber security, where one of the key factors influencing risk is the external threat posed by the adversary. A topical benefit would be appreciation of the data theft variable in modern ransomware attacks and how this influences the overall impact and therefore risk for your organization.
- **Brainstorming** – this is an imaginative thinking technique that is commonly a group exercise. Brainstorming has the intended benefit of helping to generate new ideas, maximize group knowledge, and promote out-of-the-box thinking that would normally be limited if conducted alone. The inclusion of a diverse range of views in risk assessments can have many benefits and is commonly done in threat landscaping exercises.

The use of structured analytic techniques can help to ensure any risk assessments you make are more structured and transparent. They also help you maximize the thought potential of your teams. You may question the importance of transparency in making risk assessments, but this can be invaluable to help you identify improvements and avoid mistakes or missteps.

Another lesson from the field of intelligence is the strength of cognitive diversity. Structured analytic techniques help you to promote diverse thinking and get the most out of your existing team. However, there is a limit to the ability of each individual and building cognitively diverse teams is an important step to avoid collective bias. The hiring of a diverse range of analysts is something that traditional intelligence has historically struggled with, but one it has looked to rectify in recent years.

Matthew Syed covers the concept of cognitive diversity well in his book, [Rebel Ideas](#), in which he advocates the need for building a team of rebels to help solve complex problems – of which you can be sure cyber security risk assessment is one.



1. An intelligent individual – limited to their own knowledge subset



2. A team of clones = lots of smart individuals who think in the same way



3. A team of rebels – no smarter than the team of clones, but they have wider coverage and tend to look at challenges from different perspectives



4. Rebels without a cause. Like the team of rebels – but they aren't working in synergy



5. Diverse team with dominance. Team members only say what they think the leader wants to hear



6. Team begins to parrot leader – a team of rebels becomes a team of clones

As seen in scenario three, a team of rebels, or a cognitively diverse team, has a better opportunity to cover the full problem space for complex issues. As we have touched upon already in this article, a risk assessment involves a complex number of variables, and having expertise with different frames of reference across these will be valuable to ensure you make the best assessment.

Put plainly, you need to ensure the process you set up to conduct risk assessments pulls on different frames of reference and expertise within your organization. If there is an area of expertise or reference that your team does not cover, then factor that confidence in to your assessments and look at how you may be able to make up for that; for example, by bringing in consultancy services.

In simpler terms, **the intelligence field has spent time understanding the psychology of making judgements and developed ways to account for human cognitive limitations and pitfalls.** The benefits to you of implementing these lessons in risk assessments are:

- **Improved consistency across your risk assessments,** which enables you to make better-informed decisions about where and how to prioritize investment and effort.

- **Minimization of bias in your assessment process,** so you have more accurate risk assessments that are not influenced by unrepresentative factors or human fallacy.

- **Maximizing the expertise of your teams** through understanding the benefits of cognitive diversity and how to maximize the use of collective team knowledge.

- **Use your data more effectively.** You will never have perfect data, but you can make the most of what you have by ensuring it is validated, and by making certain that valuable data is not discarded due to weak assumptions.

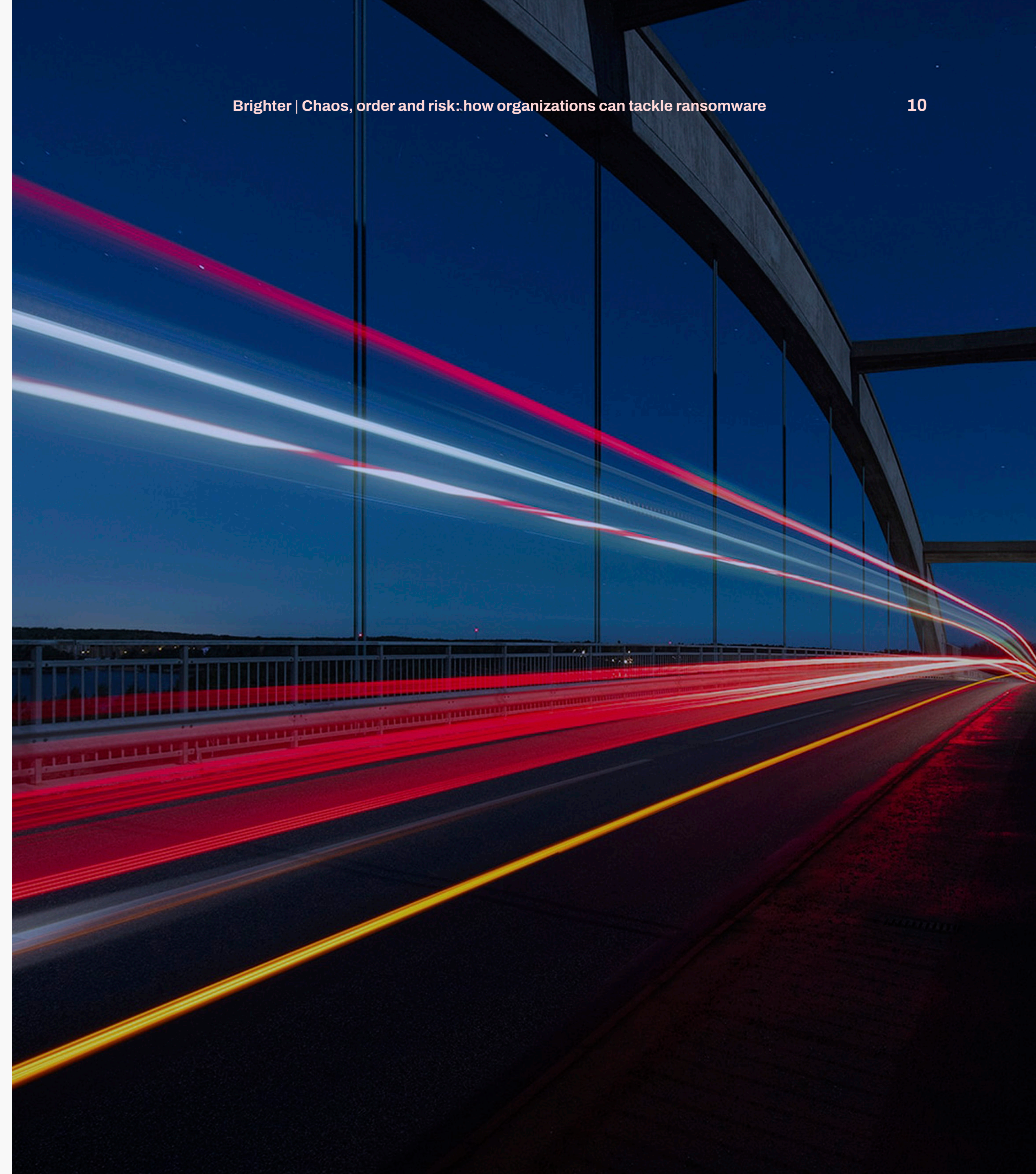
One last lesson from intelligence is emphasis on the consumer, or the end audience, of any assessment. It's incredibly important to speak the language of the audience – if you don't communicate and frame the output as something your consumers will understand, it will all be for nothing. You can implement simple, practical solutions for this, such as assigning confidence using high, medium and low, or translating these into percentages depending on what is impactful and useful for the end consumer.

Conclusion

Returning to our original question: what is the risk of ransomware to your organization? This article identifies an approach that can help you answer this question in a structured and analytical manner. The tools included in this article – as well as the wider reference material – provide a baseline for building a risk-assessment process that will produce higher-quality end determinations.

Building a qualitative risk-assessment process will ensure there is consistency and transparency that will give you and your stakeholders confidence in your outputs. You cannot control the variables that influence the risk, but you can control the process you use to assess the risk.

We have spoken at a simple level of assessing the risk through factoring in the impact and probability, but you should at least also include the threat and the existing mitigating controls of your organization. Understanding these factors is not only important for this question but also the next one – working out where you should invest to protect your organization.



Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

