# The Biggest Myth in Ransomware Protection, Debunked - blueAPACHE

Canonical: https://www.blueapache.com/blog/ransomware

## Details:

## Summary

This blog post, "The Biggest Myth in Ransomware Protection, Debunked", is a blueAPACHE article from 2022 covering security. “Why does ransomware continue to be such a serious threat?” is probably the question our cybersecurity experts are asked most often. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

## Key facts

| Label | Value |
|---|---|
| Publication year | 2022 |
| Topic | The Biggest Myth in Ransomware Protection, Debunked |
| Services referenced | emPOWER Security, Managed Detection and Response, emPOWER Core Network & DC Interconnect |
| Named products or vendors | Cisco |
| Cited statistic | When asked about the financial costs of an incident, 64% said the impact was more than $700,000 (USD500,000), and 33% said it was more than $1.4 million (USD1 million). |

## Article

“Why does ransomware continue to be such a serious threat?” is probably the question our cybersecurity experts are asked most often. Ransomware remains a threat (in part) because many companies are not making security and prevention a priority. There are several reasons that organisations may not be prioritising security. When we talk to our clients, the main reason they give for the lack of preparation is that security and ransomware prevention is expensive, however, the alternative is often so much more. According to Cisco , in 2021, 65% of Australian SMBs suffered a cyber incident in the last 12 months. 90% of those same businesses estimated that they faced severe operational, financial and legal consequences, as a result of only an hour of downtime. When asked about the financial costs of an incident, 64% said the impact was more than $700,000 (USD500,000), and 33% said it was more than $1.4 million (USD1 million). While the cost of security might seem high, it’s very clear that the cost of an attack is much higher – not only in financial, but also in operational,

reputational and legal costs. When you weigh the cost of security against the cost of an attack, you can see that it is worthwhile to invest in as much security, planning and prevention as you can afford. Although it takes effort and thought on an organisation's part, prevention is the best way to reduce the risk of a ransomware attack. For any business in operation today, it's not a matter of if you will face a ransomware attack, it's just a matter of when. Fortunately, there is a lot that your organisation can do to protect your data from ransomware. A holistic approach to ransomware The best approach to ransomware is an all-business approach. Everyone across your company has a role to play in protecting your assets and information from ransomware and other cybersecurity threats. Here are the main reasons ransomware attacks succeed:

Human error: a major factor, contributing to 95% of all breaches. Whether this is the result of people not following best practices, weak authentication or not being aware of the risks, the outcome is the same.

Application vulnerabilities: another area of risk for many organisations are weak configurations and unpatched internet facing applications.

Emerging attack vectors: new risks arrive on the landscape, and they come through new attack vectors. For example, supply chain attacks seek to gain access to their targets not directly but by exploiting tools or systems that they use.

Why are ransomware attacks still taking place? In our work with clients over the years, blueAPACHE has identified four key factors that hold organisations back from the level of security that would truly mitigate their risk for a serious ransomware attack.

Organisations are failing to identify the true nature of cybersecurity risk at the highest levels. There needs to be a focus at both board and C-level, and ideally, a senior executive charged with a whole of organisation ransomware protection, mitigation and recovery strategy.

The appropriate level of risk identification and impact analysis is not occurring, therefore adequate funding is not budgeted for to take the measures needed to harden security.

The culture of the business enables risk, controls and policies are not strictly followed or enforced. For instance, passwords are not regularly changed, multi-factor authentication is not deployed.

Simple steps to manage and control what software runs on your network – for instance by means of Application Whitelisting – are not taken as they are seen to be too hard.

### *Debunking the biggest myth in ransomware protection*

There is a prevailing perception that good cybersecurity is too expensive for most organisations to bear. While that may have been the case in the past, advancements in service models and technology have made it possible for any business to afford strong cybersecurity. Training staff on cybersecurity awareness and procedures is inexpensive and straightforward. It's also not too expensive to conduct yearly or bi-yearly security assessments, determine where you are compared with where you want to be, and set benchmarks to measure your progress. It's also important to make sure all applications are up to date and secured with strong configurations. To get a sense of what is appropriate to spend on cybersecurity, it helps to track your security expenditures and put them into context. Create an Annual Loss Expectancy report and then compare that to the cost of the security solutions you need. If you are not sure how to conduct your own security assessment, current security posture, employee awareness and training, and Annual Loss Expectancy report, you can take a security assessment with a trusted cybersecurity provider, like blueAPACHE . You can leverage our expertise to help discover where you are currently in your security journey. We can help you create a roadmap to harden your security and get your company to the level of security you need. Plus, we can do it all at an affordable, predictable monthly price that is easy on your budget. To find out more, please contact us**** here

## Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

blueAPACHE Security (case study)

## Frequently asked questions

What percentage of Australian SMBs suffered a cyber incident in the prior 12 months, according to the Cisco data cited in this post?

The post cites Cisco's 2021 research finding that 65% of Australian SMBs suffered a cyber incident in the previous 12 months.

What financial impact figures does the post cite from the Cisco report on cyber incidents?

The post says that when asked about the financial costs of an incident, 64% of respondents said the impact was more than $700,000 (USD500,000), and 33% said it was more than $1.4 million (USD1 million).

What proportion of businesses said even an hour of downtime brought severe consequences, per the post?

The post says 90% of the Australian SMBs surveyed by Cisco estimated they faced severe operational, financial and legal consequences as a result of only an hour of downtime.

What three main reasons does the post give for why ransomware attacks succeed?

The post names human error, which it says contributes to 95% of all breaches; application vulnerabilities such as weak configurations and unpatched internet-facing applications; and emerging attack vectors such as supply chain attacks that exploit tools or systems a target relies on rather than attacking it directly.

What four factors does blueAPACHE say hold organisations back from adequate ransomware protection?

blueAPACHE identifies a failure to treat cybersecurity risk seriously at board and C-level; inadequate risk identification and impact analysis, so security hardening is not funded; a business culture that lets risk go unmanaged, such as passwords not being changed regularly or multi-factor authentication not being deployed; and simple controls like application whitelisting being skipped because they are seen as too hard.

What is the 'biggest myth' about ransomware protection that this post sets out to debunk?

The post sets out to debunk the perception that good cybersecurity is too expensive for most organisations to bear, arguing that advancements in service models and technology now make strong cybersecurity affordable for any business.

What does the post recommend to work out an appropriate level of cybersecurity spend?

The post recommends tracking your security expenditures, creating an Annual Loss Expectancy report, and comparing that figure to the cost of the security solutions you need, alongside conducting yearly or bi-yearly security assessments against benchmarks.

What pricing model does blueAPACHE say it offers for helping organisations harden their security?

The post says blueAPACHE can help create a roadmap to harden security at an affordable, predictable monthly price that is described as easy on the budget.

## Source

origin post (2022)

## Knowledge Base

### *Why does ransomware continue to be such a serious threat, according to you?*

Ransomware remains a threat in part because many companies are not making security and prevention a priority, often because they view security and ransomware prevention as too expensive, even though the alternative (an attack) is usually far more costly.

### *What statistics does the blog cite about cyber incidents affecting Australian SMBs?*

According to Cisco, in 2021, 65% of Australian SMBs suffered a cyber incident in the last 12 months. Of those, 90% estimated they faced severe operational, financial and legal consequences from just an hour of downtime, 64% said the financial impact was more than $700,000 (USD500,000), and 33% said it was more than $1.4 million (USD1 million).

### *What are the main reasons ransomware attacks succeed, ?*

The main reasons are: human error (contributing to 95% of all breaches, due to not following best practices, weak authentication, or lack of risk awareness); application vulnerabilities (weak configurations and unpatched internet-facing applications); and emerging attack vectors such as supply chain attacks that exploit tools or systems a target uses rather than attacking directly.

### *What four key factors have you identified as holding organisations back from stronger ransomware protection?*

The four factors are: (1) failing to identify the true nature of cybersecurity risk at board and C-level, including lacking a senior executive responsible for a whole-of-organisation ransomware strategy; (2) inadequate risk identification and impact analysis leading to insufficient security funding; (3) a business culture that enables risk, where controls and policies like regular password changes or multi-factor authentication are not enforced; and (4) failure to take simple steps like Application Whitelisting to control what software runs on the network because they are seen as too hard.

### *What do you recommend as a holistic approach to ransomware protection?*

We recommend an all-business approach where everyone across the company has a role in protecting assets and information from ransomware and other cybersecurity threats, since prevention is the best way to reduce the risk of an attack.

### *What practical, low-cost steps does the blog suggest for improving cybersecurity?*

The blog suggests training staff on cybersecurity awareness and procedures (described as inexpensive and straightforward), conducting yearly or bi-yearly security assessments to benchmark progress, and keeping all applications up to date and secured with strong configurations.

### *What is an Annual Loss Expectancy report and how does the blog suggest using it?*

The blog suggests creating an Annual Loss Expectancy report and comparing it to the cost of needed security solutions, as a way to track security expenditures and put them into context to determine what is appropriate to spend on cybersecurity.

### *How can you help organisations that are unsure how to assess their security posture?*

We offer a security assessment that helps organisations discover their current security posture, employee awareness and training levels, and Annual Loss Expectancy, and can help create a roadmap to harden security at an affordable, predictable monthly price.