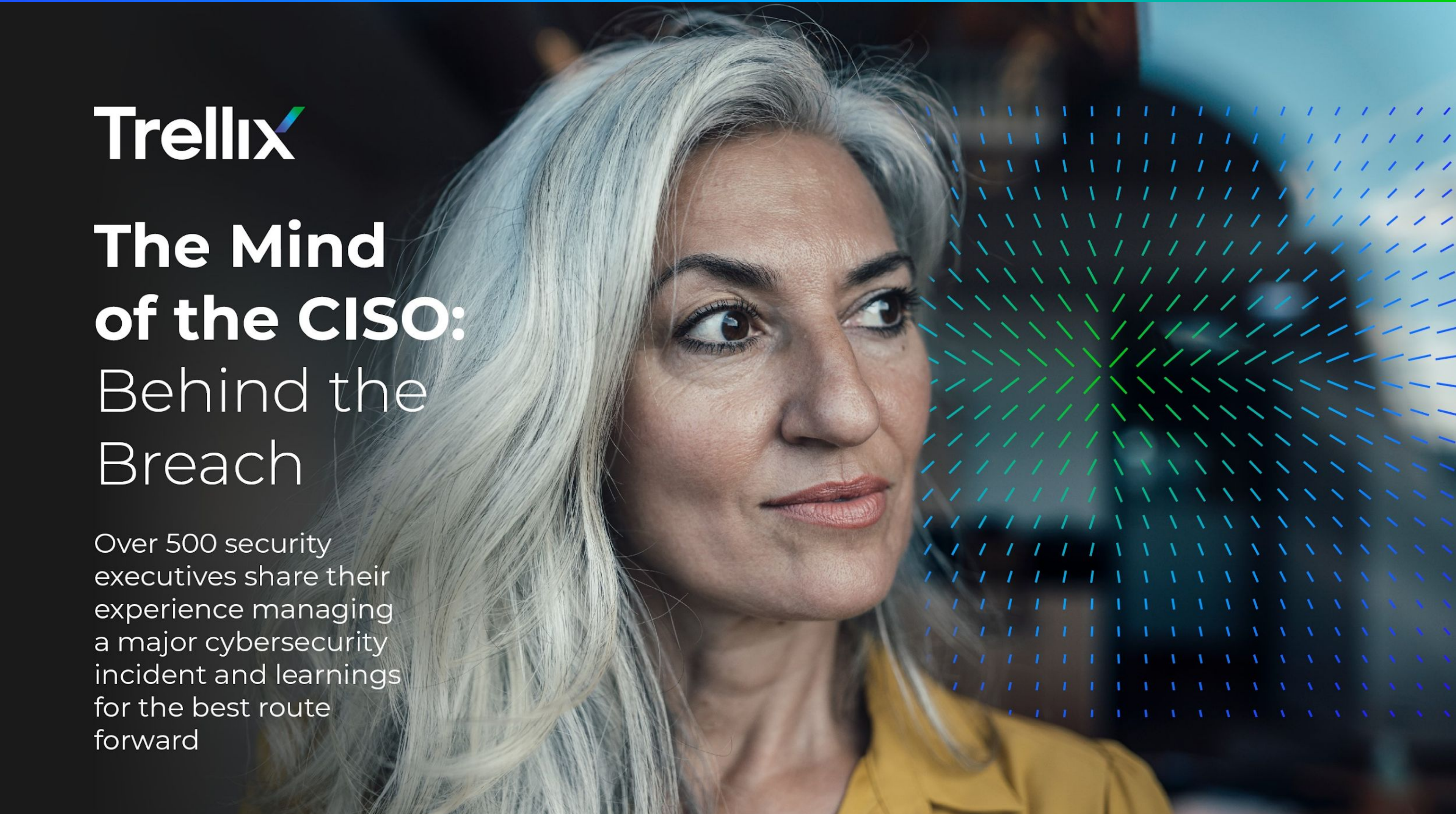
Trellix

The Mind of the CISO: Behind the Breach

Over 500 security executives share their experience managing a major cybersecurity incident and learnings for the best route forward



Manage Multiple Major Incidents Over 5 Years

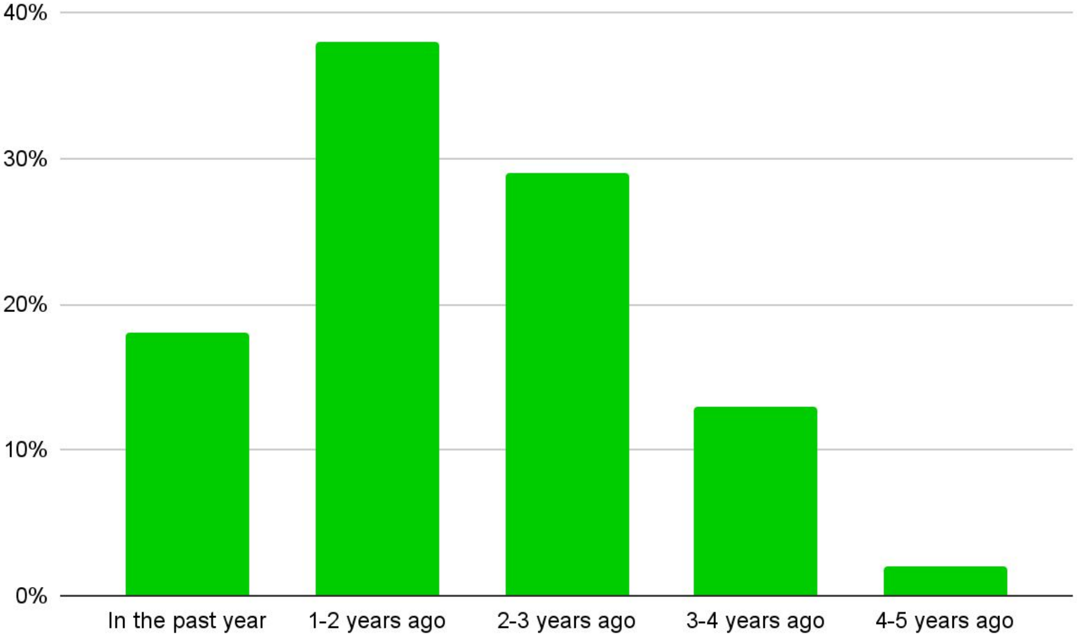
63%

have managed more than one major cybersecurity incident within the last 5 years in their role as CISO

37%

have managed just one major cybersecurity incident within the last 5 years in their role as CISO

In the past five years, have you experienced managing a major cybersecurity incident (e.g. loss of valuable data, reputational loss, etc.) for your current organization, or any previous organizations when in a CISO role? [500]



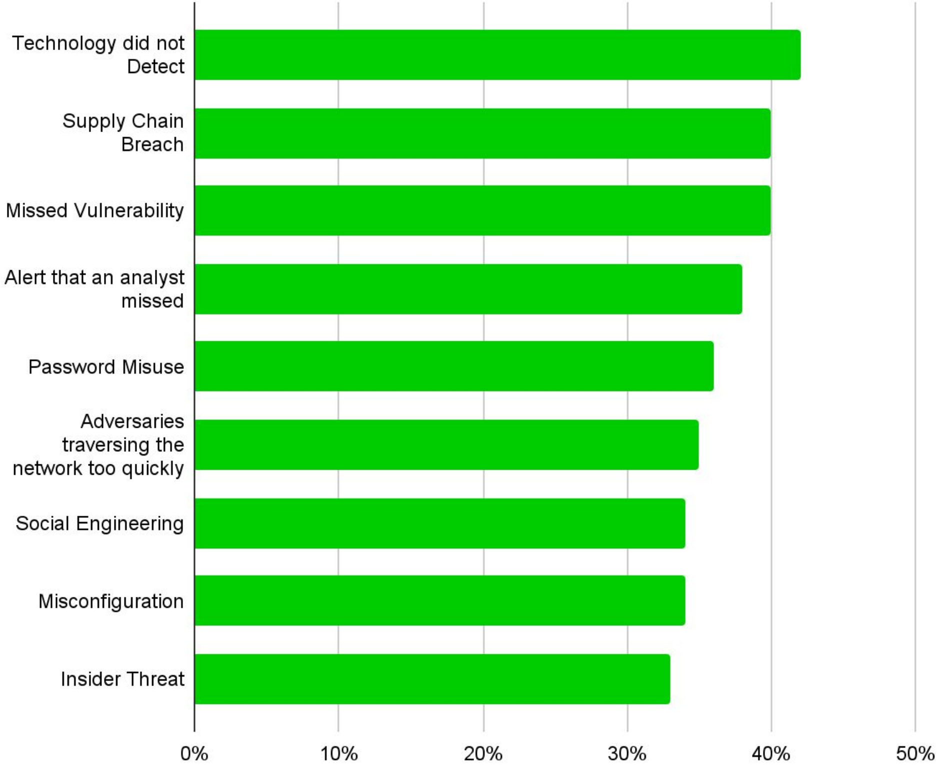
On average CISO's managed their most major cybersecurity incident within the last 2 years.

Respondents Selected 3 Causes as Reasons for the Major Incident

"they were able to **impersonate** that SVP and approve a false invoice"
"the initial point of attack that they got in was a very old server and **it's almost impossible to secure a server that old against modern techniques and modern tools.**"
CISO, Manufacturing, USA

"she was new at the company, she'd been there less than a year, **she hadn't been through all of our training**"
CISO, Manufacturing, USA

"**We couldn't tell where the attack was coming from**, it took a good, few hours. We couldn't understand or couldn't **detect** the tools they were using, where they were coming from"
CISO, Manufacturing, UK

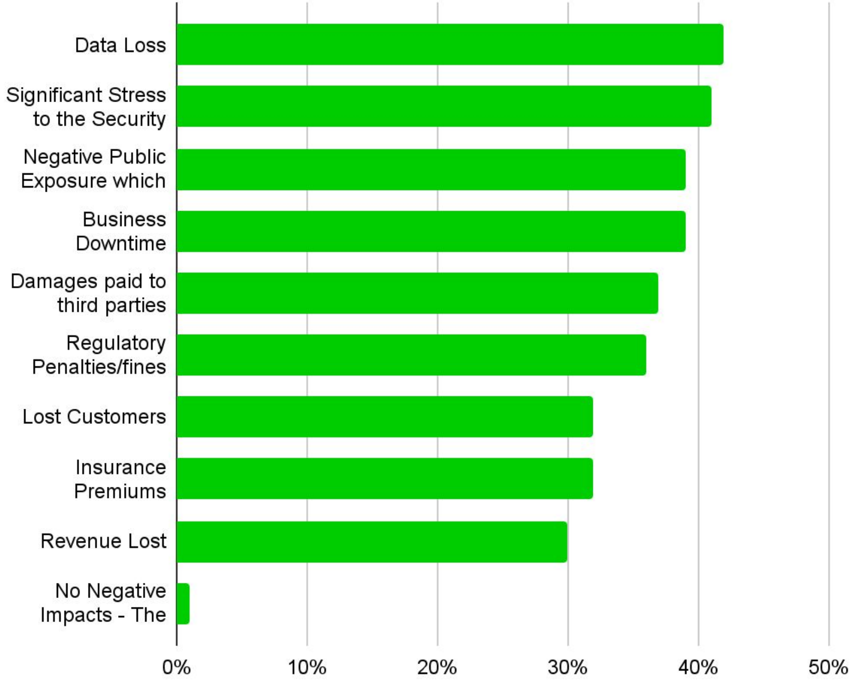


Top Impact of Major Incident: Data Loss

“Just the breach alone cost, with fines and everything, **about $6million but with the reputational risk and everything, it was around $25million dollars**"
Director of Security Operations, Public Healthcare, USA

"**Constant vigilance** and watching. Some **additional overheads**, some **additional costs**, things like that were the main impacts"
CISO, Manufacturing, USA

“Even if customers or businesses say, “It’s all fine, you handled it very, very well”, in the back of their minds, there’s always this… **how can we rely on this organisation? What if it happens again?**"
CISO, Manufacturing, UK

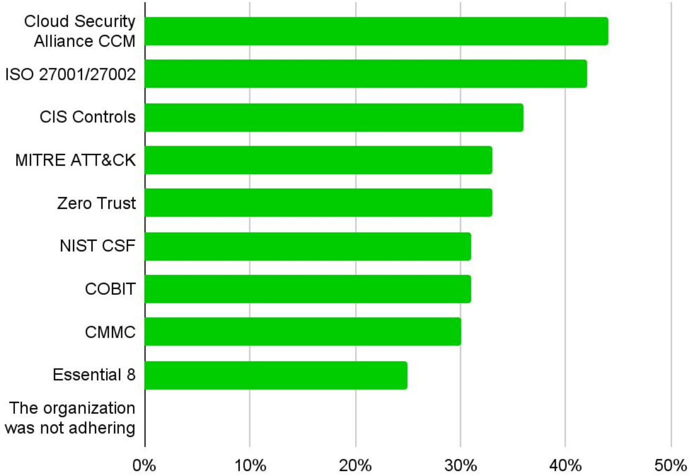


What impact(s) did the major cybersecurity incident that you managed have on the organization? [500] Not showing all answer options

100% Adhered to at Least One Framework

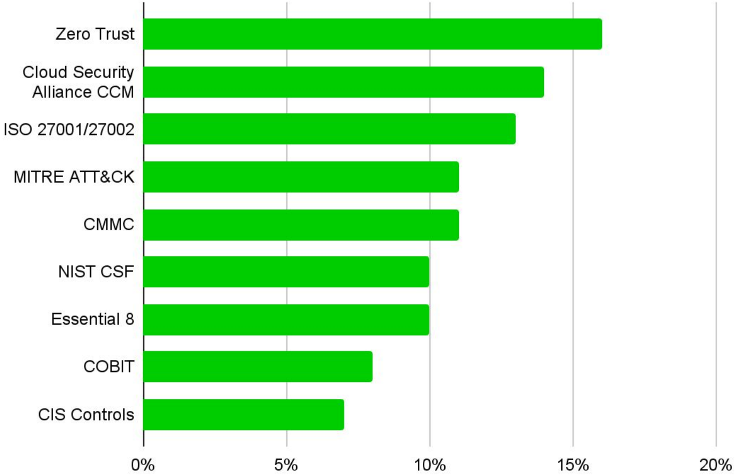
Major Incident Managed in the Last 2 Years

Frameworks adhering to at the time of the incident



What cybersecurity framework(s) was the organization adhering to at the time of the major cybersecurity incident? [500] Not showing all answer options.

Prioritized framework by importance in managing incidents



Please rank the following frameworks based on your view of their importance in managing cybersecurity incidents. [500] Showing responses ranked first, not showing all answer options

CISOs Adapt and Learn From Prior Incidents

Approach to Cybersecurity is More Cyber-Resilient

91%

felt their resilience improved as a result of the incident

74%

felt their approach to cybersecurity is 'never trust, always verify' as a result of the incident

91%

felt their approach to cybersecurity is more cyber-resilient since the incident

"You're never as secure as you would like to think you are right, and **you have to look in the darkest crevices and the smallest cracks because that's where the weakness lies**"
CISO, Manufacturing, USA

"Just reinforced the concept that we need to be ever-vigilant and **no matter how secure we think we've gotten things, no matter how many tools we have in place, it's a constant battle**"
CISO, Manufacturing, USA

To what extent do you agree or disagree with the following statements? [500] Showing combination of those that selected 'agree' or 'strongly agree'

XDR: Potential to Prevent Incidents

76%
believe that if they had XDR, the major cybersecurity incident would have had a lesser impact

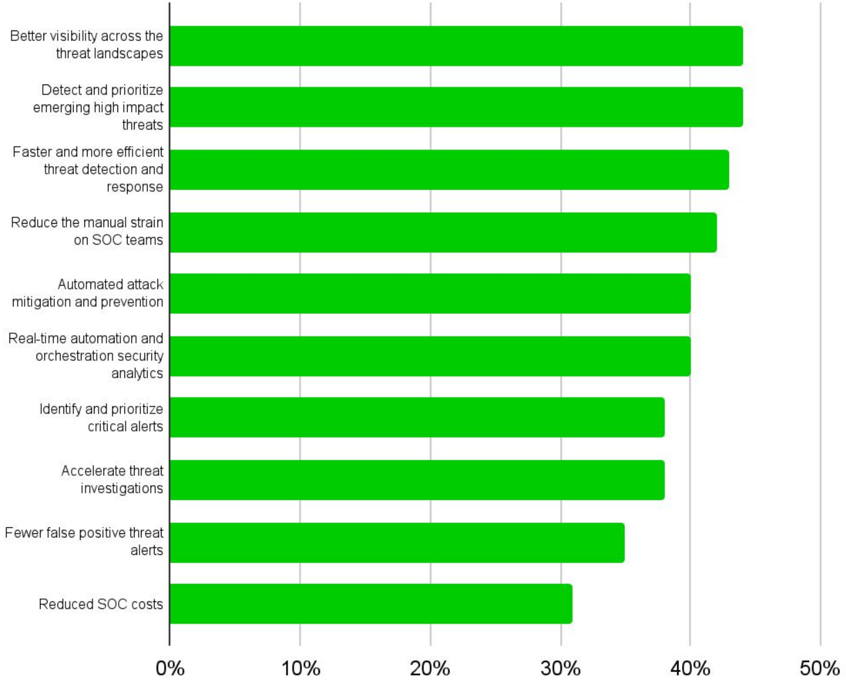
95%
believe that if they had XDR, the major cybersecurity incident would have been prevented

"If we had **true correlation** across all the tools, **would we have caught it earlier?**"
CISO, Manufacturing, USA

"Oh, if I had that then, number one, **the email wouldn't have gotten through the filtering systems**"
CISO, Government Agency, Australia

Based on your understanding of XDR as a platform that connects your tools, to what extent do you agree or disagree with the following statements? [267] asked to respondents that were not using XDR at the time of the incident. Showing combination of those that strongly agree and slightly agree.

CISOs Recognize XDR Benefits



“Because **we use multiple systems,** 1,000s of systems, **we needed to assess quickly which ones were vulnerable** to this particular vulnerability, and what do we do about them"
CISO, UK

"One of the lessons that **technology is always vulnerable** and while companies have limited budgets, outside **there might be unlimited opportunities for hackers**”
CISO, UK

When considering an Extended Detection and Response (XDR) solution, what benefits would you look for it to include? [500] Not showing all answer options.

Trellix