EXECUTIVE SUMMARY

2024 State of Zero Trust & Encryption Study

Sponsored by Entrust

Independently conducted by Ponemon Institute LLC

Publication Date: May 2024

ENTRUST
SECURING A WORLD IN MOTION

Ponemon INSTITUTE

INTRODUCTION

Our threat landscape continues to intensify from AI-generated deepfakes and synthetic identity fraud through nation-state attacks and cyber warfare. With that lens, the Entrust Cybersecurity Institute is pleased to highlight the results of our 18th annual study with the Ponemon Institute that delves into the state of Zero Trust and encryption in 2024.

For this study, the Ponemon Institute surveyed 4,052 IT and IT security practitioners across the United States, United Kingdom, Canada, Germany, Australia and New Zealand, Japan, Singapore, and the Middle East.

Contents

Cyber Risk Influencing Opinions About Zero Trust

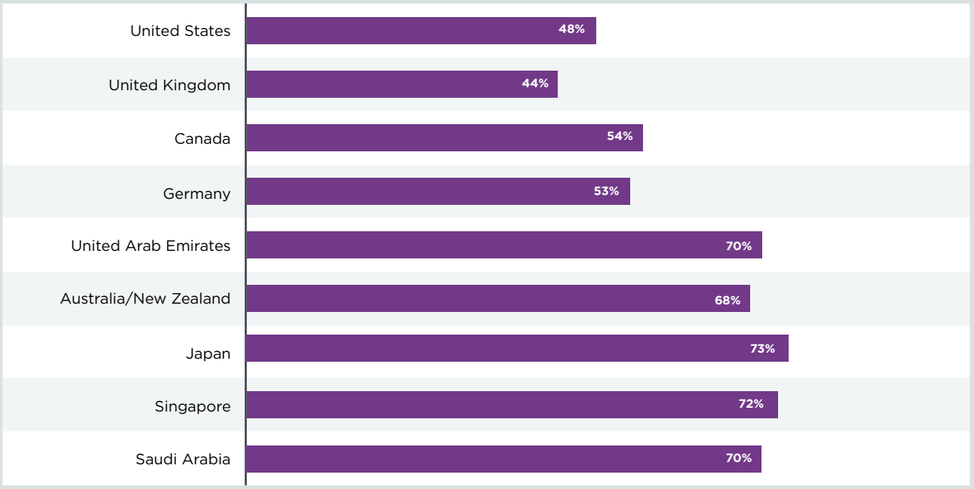
The risk of a cyber breach is the No. 1 global driver for Zero Trust strategy implementation cited by 37% of respondents, followed by the expanding attack surface at 30%. This pattern is even more pronounced in the U.S., with 50% of organizations citing cyber breach risk and 29% reporting the expanding attack surface for a combined total of 79%.

Regulations and standards are a consistent third driver for Zero Trust adoption at 29% globally, which is still significant. It is interesting to note that the U.S. is the outlier at only 18%, which also likely highlights the lower regulatory bar in the U.S., especially at the federal level.

Zero Trust Adoption Under Way, But West Lagging

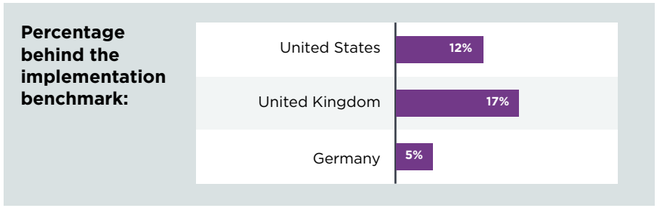
61% of organizations have begun their own Zero Trust journey. However, the U.S. and other Western countries are lagging in the global adoption benchmark.

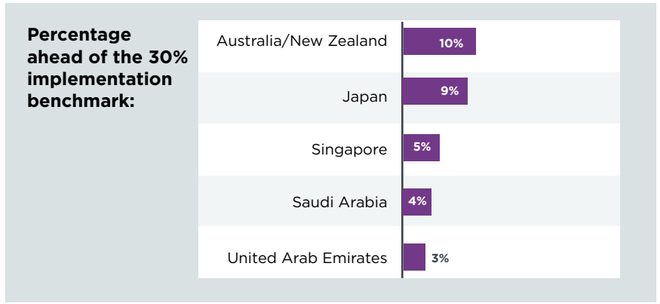
Percentage of organizations that have adopted Zero Trust per country



Zero Trust Adoption Cont’d

This adoption pattern is even more pronounced when looking at the global numbers for partial Zero Trust principle implementation (12%) and full Zero Trust principle implementation (18%). Apart from Canada, the surveyed countries in the Western Hemisphere lag the combined 30% global Zero Trust implementation benchmark by up to 17%.





With the U.S. and other Western countries lagging global Zero Trust adoption and implementation benchmarks, this raises the concern that a majority of Western entities know they have a problem but are unable to adopt Zero Trust for one reason or another – leaving them vulnerable.

Do Organizations Have Senior Leadership Support for Zero Trust?

Close to 60% of organizations around the globe report significant or very significant senior leadership support for an enterprise-wide Zero Trust strategy, and this number is very consistent across the surveyed countries. This is good news for CISOs, or is it?

At the same time, the top two cited Zero Trust implementation challenges are a lack of in-house expertise and adequate budget, both of which are largely within an organization's control through funding for resources, tools, and training. Except for Germany and the Middle East, lack of in-house expertise was cited as the top one or two challenge to Zero Trust implementation. In the U.S., a full 60% reported lack of in-house expertise as the top problem, with inadequate budgets a recurring theme across the U.S., UK, Canada, and Germany.

Despite consistent senior-level support for an enterprise-wide Zero Trust strategy relative to the 59% global benchmark, Australia/New Zealand, Japan, and the Middle East all cited lack of leadership buy-in as their No. 2 challenge to implementing Zero Trust.

Navigating the Zero Trust Journey

Regardless, CISOs are pressing forward. At the outset of the Zero Trust journey, it can all seem a little daunting – where to start, what to prioritize, which vendor solutions to select, and so on. Identities are cited as the risk area with the highest priority for an organization's Zero Trust strategy by 40% of global respondents, followed by devices at 24%. This pattern was very consistent across the surveyed countries.

Also, best-of-breed solutions are cited as the most important capability needed to support an organization's Zero Trust strategy by 44% of respondents, followed by an integrated ecosystem of one to three vendors by 22%. Again, this response was relatively consistent across countries but also highlights the delicate balancing act being asked of today's CISOs to use best-of-breed solutions while also keeping the vendor count down.

Top Breach Concerns of Respondents

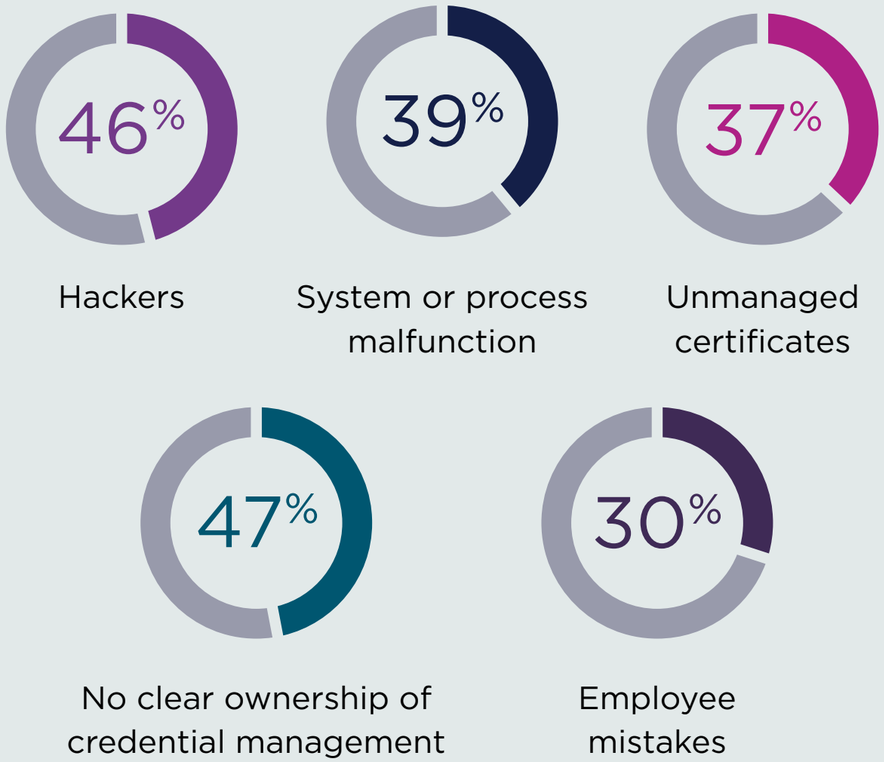
Always a perennial concern, hackers leapt to the top of the list in FY23 cited as the top worry by 46% of respondents for the exposure of sensitive or confidential data. This is just another reminder of the intensifying threat landscape and the need to employ good cyber hygiene with the adoption of a Zero Trust strategy.

System or process malfunction came in second again, cited by 39% of respondents in FY23, up 7% year over year – unfortunately, not that surprising given other reported contributing factors including increasing system and network complexity, proliferation of credentials to manage, a critical shortage of skills and resources, and in many cases unclear ownership.

Related to the above, unmanaged certificates were cited as a top three security concern by 37% of respondents, with 47% indicating no clear ownership of credential management as a key pain point. This highlights the need for effective certificate lifecycle management with clear ownership.

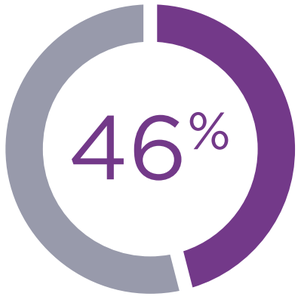
A welcome surprise is that for the first time, employee mistakes did not make the top three list of concerns. Dropping from 54% in FY19 to 47% in FY22 to 30% in FY24, this is a good sign that phishing-resistant identities coupled with increased cyber awareness and education are paying off.

Top breach concerns reported in FY24:

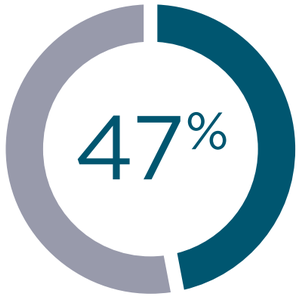


Solving the Perennial People, Skills, and Ownership Problem

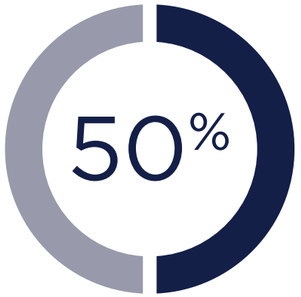
With the intensifying threat landscape and more and more things to secure, CISOs and their teams are feeling the crunch. Respondents reported the key reasons credential management is so painful in FY24:



said insufficient personnel



reported no clear ownership



cited a lack of skilled personnel

Get the Full Report

Learn more about implementing an effective Zero Trust strategy by downloading the full Ponemon 2024 State of Zero Trust & Encryption Study.

Download Report

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION