THALES
Building a future we can all trust

2022 Thales Data Threat Report

Critical Infrastructure Edition

#ThalesCIReport

cpl.thalesgroup.com

Introduction

Critical infrastructure, which for the purposes of this report includes energy/utilities, telecommunications, transportation and trucking/shipping companies, became top of mind for many beginning in 2020 when high-profile security attacks impacted millions of people across the globe. From the ransomware attack that compromised a major U.S. gas pipeline in 2021 to the rise of nation-state attacks, particularly since the onset of the Russian invasion of Ukraine, critical infrastructure organizations are under siege.

The effects of cyberattacks on critical infrastructure are not only inconvenient, but they can also be life-threatening. Critical infrastructure organizations have some of the highest uptime requirements due to health and human safety concerns, resulting in even higher availability requirements than banking or healthcare. Security breaches in this sector can be incredibly disruptive to society and are attracting considerable attention from governments and regulatory bodies around the world.

We summarize some of the most important findings of the 2022 Thales Data Threat Report Critical Infrastructure Edition, which includes responses from 300 security leaders and practitioners within critical infrastructure organizations and conclude with thoughts on reducing the risk of attacks such as ransomware and malware.

451 Research

S&P Global
Market Intelligence

Source: 2022 Data Threat custom survey from 451 Research, part of S&P Global Market Intelligence, commissioned by Thales

Contents

Remote Working Worsens the "Human Factor" Weakest Link

Unsurprisingly, the "human factor" remains the weakest link in cybersecurity. A majority of successful malware and ransomware attacks gain an initial foothold in organizations due to user error. This includes using easily guessed passwords and falling victim to phishing and socially engineered techniques such as business email compromise. This situation has worsened due to large-scale shifts to "hybrid" working arrangements that constitute some combination of working remotely and in traditional offices and often varies from worker to worker. Additionally, the convergence of Information Technology (IT) and operational technology (OT) makes it easier for attackers to move laterally within organizations, turning IT problems into much more impactful OT system issues.

The convergence of Information Technology (IT) and Operational Technology (OT) makes it easier for attackers to move laterally within organizations, turning IT problems into much more impactful OT system issues."

In a stacked ranked survey, respondents were asked to prioritize their perceptions of the greatest threats facing their organizations. Respondents prioritized accidental incidents (human error), hacktivists, cybercriminals and nation-state actors as their top four threats. More than three-quarters (79%) of respondents were very or somewhat concerned about security risks and threats from employees working remotely. Surprisingly, just 37% of respondents prioritized multi-factor authentication (MFA) as a security technology most effective against preventing cyberattacks, even though MFA is widely regarded as one of the best ways to counter inadvertent user error. Only 51% of critical infrastructure organizations indicated that they use MFA, 3% lower than all industries in the survey. Modern authentication, including MFA, was primarily deployed for remote/mobile non-IT employees and staff (68%) and privileged employees and IT staff (53%).

79%

of respondents were concerned about security risks from employees working remotely.

51%

of critical infrastructure organizations indicated that they use Multi-Factor Authentication (MFA).

Malware and Ransomware Attacks Increase and Become More Complex

Across all critical infrastructure organizations, 55% of respondents ranked malware as the leading source of increased security attacks, followed closely by ransomware (53%), which is logical because ransomware attacks typically include malware components. Interestingly, transportation companies reported higher malware increases than average (65%) and lower cases of ransomware (45%), while trucking and shipping reported considerably lower malware (32%) but much higher ransomware incidents (64%). Less than a quarter (19%) of critical infrastructure respondents reported having experienced a ransomware attack, compared with 20% in the overall survey. Transportation and energy/utilities respondents reported even lower ransomware attacks, at 17% each.

Criminals have realized that successful attacks against high-profile critical infrastructure organizations have a higher probability of a payoff. For example, the 2021 Colonial Pipeline attack – which stopped the pumping of oil in the Northeastern U.S. for five days, resulting in fuel shortages, panic buying and major economic impacts – cost $4.4 million in ransom ($2.4 million was later recovered). Interestingly, Colonial, along with many other victims, restored ransomed data more quickly using their own backups rather than the criminal's decryption keys and software, despite having paid the ransom.

Ransomware has changed breach economics. Given the mature, regulated nature of these industries, respondents demonstrated a stronger aversion to "harder" rather than "softer" intangible costs from ransomware. Nearly a quarter (24%) of respondents ranked financial losses, such as lost sales or penalties from lawsuits and legal expenses, as the greatest impact from a successful ransomware attack, whereas 19% cited lost productivity and 17% said recovery costs. Soft costs, including brand reputation damage, loss of customers and other long-term business impacts, trailed at only 10%, 6% and 3%, respectively, consistently lower than overall survey responses.

Critical industry respondents' willingness to pay ransom was 20%, compared to 22% of all industries surveyed; enterprises may not have a good understanding of the effects of all the parties involved, such as cyber insurance underwriters, incident response firms, government regulations and ransomware attribution. For example, NotPetya ransomware was considered an act of war by NATO, causing some cyber insurance vendors not to pay claims. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued guidance stating that facilitating ransomware payments to attackers on behalf of victims could risk violating OFAC regulations. Despite ransomware's additional impacts on data integrity and availability, the changing and unknown landscape may cause new plans to stall. Thirty-nine percent of respondents said they have no plans to change security spending, even with greater ransomware impacts.

The study also showed insufficient ransomware preparedness. Ransomware's power comes from immediate "kidnapping" of data and critical systems, requiring a rapid, rehearsed response plan. Yet only 45% of respondents have a formal ransomware plan, compared to 48% across all industries.

Criminals have realized that successful attacks against high-profile critical infrastructure organizations have a higher probability of a payoff."

Breaches and Failed Audits Are a Continuing Problem

Forty-four percent of respondents reported increases in the volume, severity and/or scope of cyberattacks in the past 12 months. More than a third (39%) of respondents experienced a security breach in the past 12 months, 6% higher than average, while 51% have experienced a breach at some point in the past, 3% higher than average.

More than a third (39%) of respondents experienced a security breach in the past 12 months."

Diverse Data Protection Strategies Need Better Alignment and Common Direction

Only 28% said they could fully classify their data."

62%

chose encryption as the best technology to protect data in the cloud.

The first step in a data protection strategy is to identify where data is stored, followed by classification, so that appropriate security protections can be employed. An impressive 57% of respondents said they have complete knowledge or are very confident they know where their data is stored, 4% higher than average. However, only 28% said they could fully classify their data, and only 49% believe they could classify at least half of their data, 6% lower than average.

Many organizations have several key management tools: 55% reported five or more and 18% more than eight. This results in considerably higher costs, complexity and risk. Responses indicated a curious gap between selecting encryption and key management. When asked to select which technologies protect data in the cloud, 62% chose encryption, while 51% selected key management. This discrepancy is likely because organizations are unaware of how their keys are managed. For example, AWS S3 encryption largely abstracts key management, so users may be unaware of how their keys are managed. A focus on key management rather than simply deploying encryption to "check a box" is critical because improper key management can lead to vulnerabilities and successful attacks – encryption is only as good as the keys in use (and how they are managed).

Security concerns about quantum computing continue to increase; only 2% of respondents have no concerns about quantum-related risks. Key concerns include future decryption of today's data (52%), risk of network decryption (56%), risk of blockchain attack (49%) and key distribution (46%).

Zero Trust Adoption Continues, Particularly in Cloud Environments

Critical infrastructure organizations typically have highly distributed infrastructures that include warehouses, shipping ports, power lines, trucks, transmitting sites and railroad assets. Adopting zero trust principles can be a key strategy by ensuring "least privilege" access to highly distributed, high-value data and assets. The transition of OT from proprietary, dedicated connections to internet of things (IoT) has greatly increased the size, complexity and elasticity of underlying networks while greatly increasing attack surfaces. These environments are generally well served by zero trust strategies.

Only 30% of respondents have a formal zero trust strategy and have actively embraced zero trust policies, while 26% have a zero trust strategy in planning and research stages and 22% have no formal zero trust strategy at all. Unsurprisingly, organizations with a formal zero trust strategy are less likely to have been breached. These track closely with the overall averages.

When asked where respondents expect to use zero trust principles, 61% of respondents plan to use zero trust in cloud access, and 53% plan to use zero trust for on-premises access and remote access management.

30%

of respondents have a formal zero trust strategy and have actively embraced zero trust policies.

20%

of respondents worldwide said they have paid or would pay a ransom for their data.

Cloud Apps and Data Continue To Grow, Increasing Attack Surfaces and Complexity

In a stacked survey question, we asked respondents to identify which targets for attacks most concerned them; cloud-based storage, cloud databases, and cloud-hosted apps were the top three. A majority of respondents reported that they have more than 40% of workloads and data in the cloud; 54% reported that more than 60% of their cloud data is sensitive. Most respondents also indicated that they have more than one cloud (IaaS) provider, leading to potential issues with the complexities of securing multiple cloud environments.

A majority of respondents reported that they have more than 40% of workloads and data in the cloud."

Moving Ahead

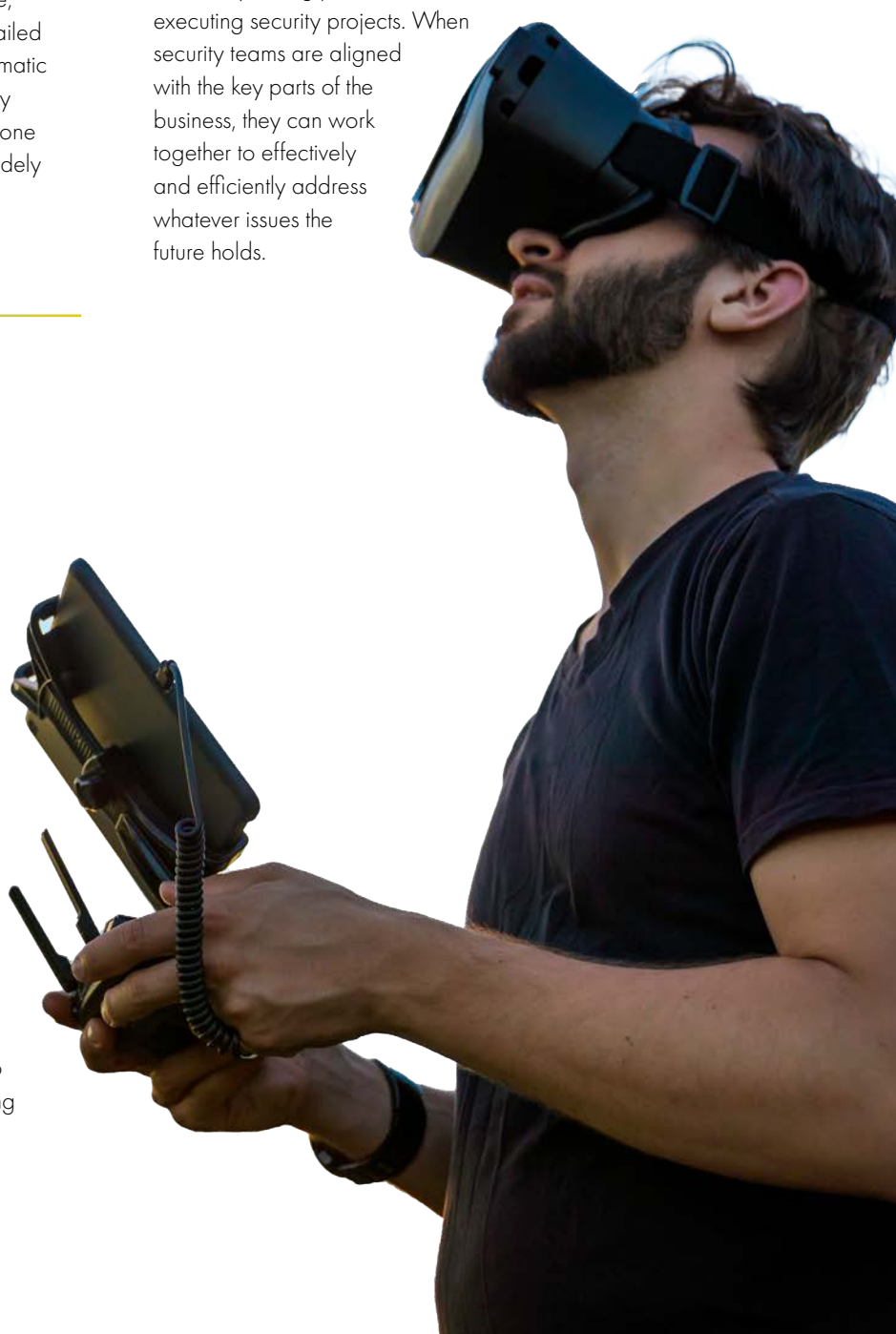
Critical infrastructure organizations have been particularly impacted by security issues due to highly distributed infrastructures, highly publicized breaches and ransomware attacks, a prevalence of exploitable IoT devices, and the human factor, which continues to be the weakest link in security defenses. Criminals seeking to breach a target need only find one human – preferably one with high privileges – using poor password hygiene or who can be tricked into releasing information, to gain a foothold. From there, ransomware, malware and other tactics can result in breaches and failed audits. Data loss from breaches continues to be problematic due to low encryption rates and overly complicated key management practices, which tend to run at odds with one another. One key defensive solution, MFA, is still not widely deployed.

Data loss from breaches continues to be problematic due to low encryption rates, overly complicated key management practices, and low deployment rates of MFA."

Zero trust continues gaining momentum, particularly in remote access and cloud environments, but a true zero trust strategy should be equally applicable to all users and devices, regardless of location. While implementing a zero trust strategy focused on users and devices outside of the organization is a fine starting point, it must be pervasive through the entire IT estate to be truly effective.

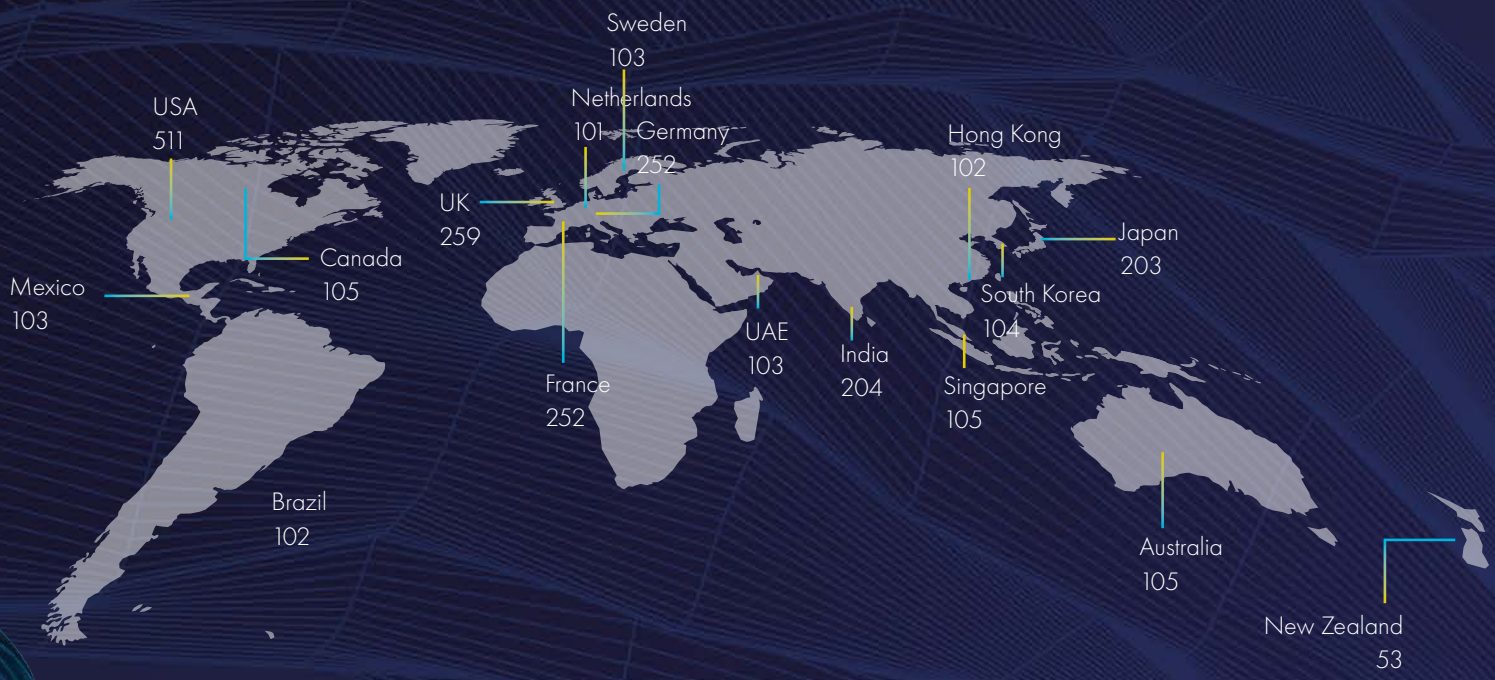
The uptake of cloud applications and data continues to trend upward, with many organizations now considering themselves "cloud-first," prioritizing cloud solutions over on-premises. Many organizations also have multiple cloud providers, which leads to difficulties in managing security cohesively across multiple cloud environments.

As organizations move forward, they'll need visibility not only across their infrastructure, but throughout their organization. Establishing a common understanding is a key part of effectively setting priorities and executing security projects. When security teams are aligned with the key parts of the business, they can work together to effectively and efficiently address whatever issues the future holds.



About This Study

This research was based on a global survey of 2,767 respondents, fielded in January 2022, via web survey with targeted populations for each country, aimed at professionals in security and IT management. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million and with US$100-250 million in selected countries. This research was conducted as an observational study and makes no causal claims. A subset of this data was created including approximately 300 respondents who identified themselves as employees of critical infrastructure organizations.

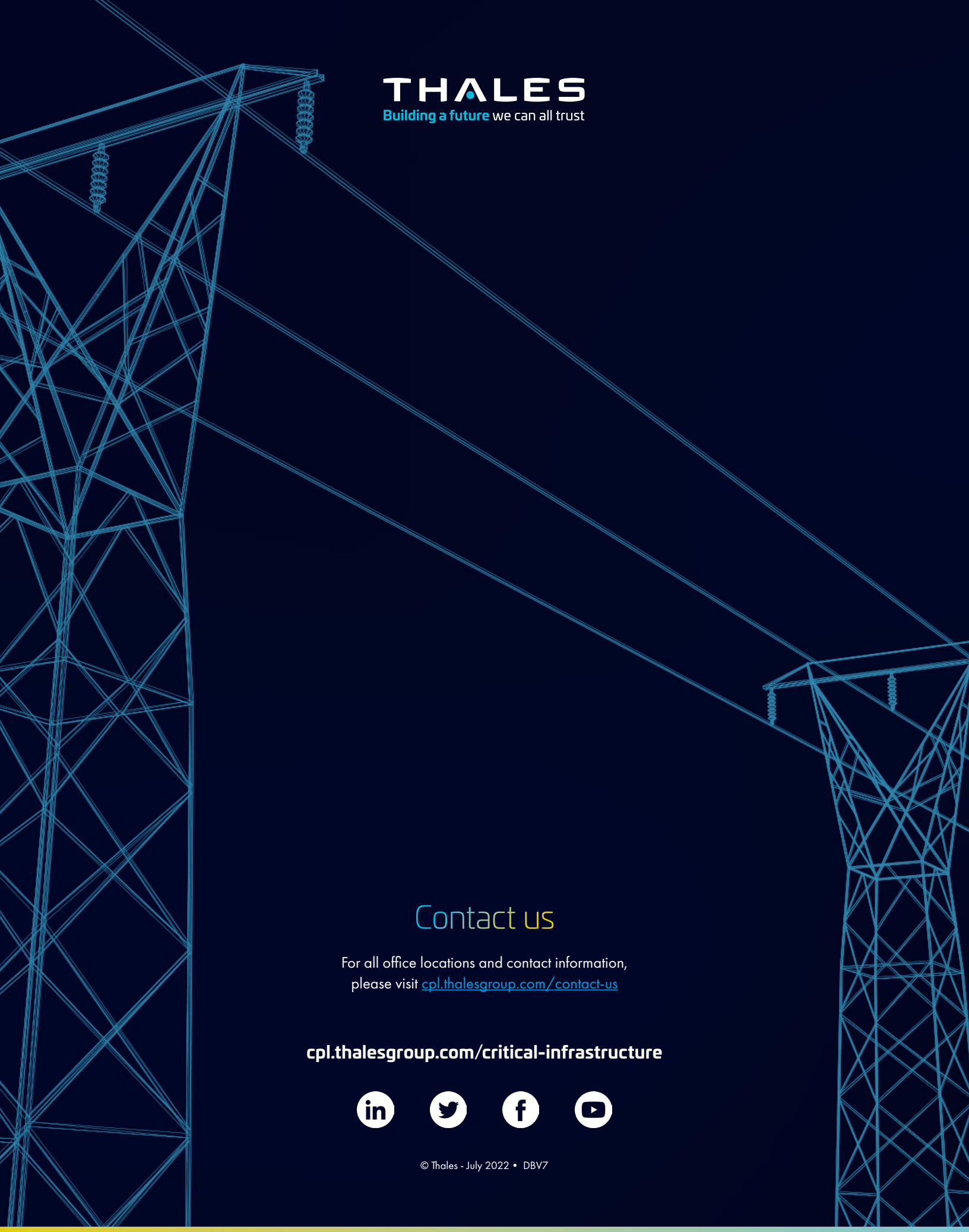


Industry Sector

Critical Infrastructure	300
Manufacturing	157
Retail	154
Technology	127
Financial Services	120
Healthcare	115
Public Sector	109
Consumer Products	107
Computers/ Electronics/Software	106
Engineering	104
Federal Government	103

Revenue

$100 million to $249.9 million	162
$250 million to $499.9 million	802
$500 million to $749.9 million	865
$750 million to $999.9 million	458
$1 billion to $1.49 billion	254
$1.5 billion to $1.99 billion	58
$2 billion or more	168



THALES
Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/critical-infrastructure