Forcepoint

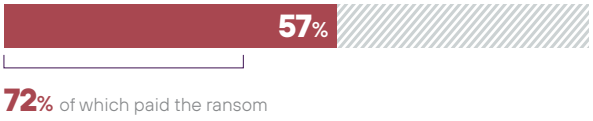
How Forcepoint can secure your Critical National Infrastructure from cyberattacks

The cyber threat landscape is fiercer than ever, and cybersecurity professionals in Critical National Infrastructure (CNI) organizations can no longer ignore the mounting pressure presented by cybercriminals.

Key findings

In our 'Panic Stations' research, with insight from 500 CNI cybersecurity professionals across the US and UK, we uncovered that 65% of CNI organizations were hit by a cyberattack in the past year. And the rate of attacks is even worse for some sectors. For example the rate increases to 75% in central government and the communications sector and 74% within energy and banking.

% of CNI organizations that fell victim to a ransomware attack



72% of which paid the ransom

On top of this, more than half (57%) of CNI organizations across both countries report falling victim to a ransomware attack in the past year, of which 72% admitted to paying the ransom.

Rapid digital transformation of IT and Operational Technology (OT) environments are compounding the challenge that cybersecurity professionals are facing.

Understandably, the occurrence of these cyberattacks are concerning for CNI cybersecurity professionals who are also battling with the challenge of securing the rapid digitally transforming IT and OT environments. Of the vital, everyday services CNI cyber professionals protect, those in the US believe power outages is of the greatest concern. Meanwhile, those in the UK feel an attack causing disruption to personal banking services would cause the greatest public panic.

Despite these differences, more than half (57%) of professionals in both territories say they fear their organization will fall victim to a cyberattack over the next 12 months.

Impact of cyberattacks on business

The impact of cyberattacks on CNI cannot be understated. For example, the infiltration of a Florida water treatment plant in 2021 presented one of the greatest risks to human life. The malicious actor's attempt to increase the sodium hydroxide to dangerous levels could have poisoned the water supply. In this case, the consequences of a successful attack would have gone beyond the company's bottom line and reputational damage to encompass the loss of thousands of lives.

Clearly, the cybersecurity measures in CNI businesses must now be top priority.

Impact of cyberattacks on employees

Cyberattacks are putting increasing strain on the people tasked to ward against them. And in today's workplace, where employee wellbeing is increasingly important and at the top of the c-suite agenda, it can affect productivity.

Our research found that the increase in cyberattacks has a negative impact on the work lives and personal wellbeing of cybersecurity professionals. Feelings of stress (35%), anxiety (39%), and burnout (37%) are affecting over a third of all CNI cybersecurity professionals. And two-fifths report the pressure to secure CNI has led them to have a low morale at work (40%), with this rising to 51% for UK employees.

The human impact of CNI cybersecurity can no longer be ignored if organizations are to maintain productive staff ready to thwart the actions of cybercriminals whenever they arise.

Steps you can take to mitigate these risks

The growing sophistication of threat actors are yet to abate, and the high-tech environment caused by the rapid transformation of IT and OT environments emboldens them. Organizations must act now to ensure resilience in the face of a high-threat landscape and high-tech digital transformation, as well as to better protect those in charge of defending vital services.

At Forcepoint, we believe this can be done by reducing the complexity for cybersecurity professionals and empowering them with the tools needed to secure new technologies alongside legacy architecture. This can be achieved in five ways:

1. Prioritize cyber hygiene

Consistently updating network security software and the safe handling of data as digitalization transforms IT and OT environments is paramount. This can prevent most low-level attacks.

2. Simplify operations

With the expanding IT and OT landscape, the number of tools cybersecurity professionals manage has increased. And this increases the risk of a potential crack in the armor. So, to reduce the number of tools needed to manage an efficient security posture, organizations must consolidate their security platform.

3. Embrace Zero Trust

Employing the "never trust, always verify" best practice will help to squash threats that have already infiltrated a network, as well as the explicit actions of employees acting maliciously.

4. Secure the route to the cloud

Utilizing a Zero Trust security posture for all inbound content arriving at the enterprise network establishes a modern air gap between connected networks and services. This mitigates the risk of embedded or concealed malware before it can enter the network.

5. Implement secure data flows

A great way to secure the flow of data between networks and devices is to create one-way data channels between trusted and untrusted networks, so data can be received, but is never permitted to exit.

How Forcepoint can help

Zero Trust Content Disarm & Reconstruction (CDR)
Enhance your cyber defenses from known and unknown threats, zero-day attacks and malware by employing our Zero Trust CDR solution. It works by extracting the valid data, verifying the information and then building brand-new data, rather than relying on only detecting malware. Learn more about this solution here.

Forcepoint ONE
This is our all-in-one, cloud native security platform that simplifies the complexity of today's cybersecurity environment by employing Security Service Edge (SSE). This solution ensures consistent threat protection to prevent malware and gives users easy access to the apps they need, without exposing the rest of the network. Learn more about this solution here.

Head here to download the full report or take a look at our critical infrastructure webpage for more information or to schedule a demo.