A Lynchpin Media
BRAND

CXO priorities

THE OT THREAT LANDSCAPE

CHALLENGES AND PRIORITIES FOR MIDDLE EAST ORGANISATIONS IN PARTNERSHIP WITH DRAGOS

DRAGOS

DRAGOS

priorities

A Lynchpin Media BRAND

CONTENTS

INTRODUCTION

OT SECURITY HAS become a key priority for CISOs and their teams in recent years, driven by digitalisation of industrial environments and the convergence of IT and OT.

While there are many advantages to digitalisation in these settings – efficiencies and improved employee and customer experience to name a few – it also throws up new challenges for IT security teams.

Attackers are all too aware of these new ‘connected’ industrial control systems (ICS) and are taking advantage, with threat groups emerging and honing their skills over periods of several years.

But OT security shortcomings can not only result in devastating reputational and financial losses, it can also mean injury and loss of life in extreme cases.

It’s vital that organisations understand the current OT threat landscape and prioritise the implementation of a robust OT security strategy to stay protected.

> **IT’S VITAL THAT ORGANISATIONS UNDERSTAND THE CURRENT OT THREAT LANDSCAPE.**

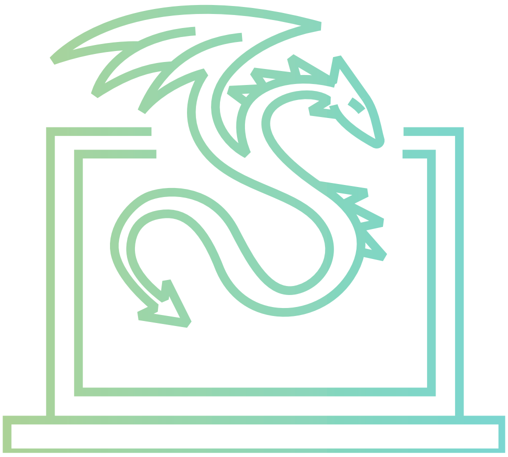
SURVEY OVERVIEW

TO FIND OUT MORE, we surveyed 50 individuals at organisations in the Middle East to find out more about the OT security landscape.

Through the survey, we aimed to discover:

- How organisations prioritise OT security – both currently and looking ahead
- The challenges organisations across the region are experiencing when it comes to OT security
- Whether budgets have been impacted by raised awareness of OT threats

DRAGOS
priorities
A Lynchpin Media BRAND



SUMMARY OF FINDINGS

- Almost **70%** respondents thought ICS adversaries posed either a medium or high to organisations in the Middle East

70%

- Management control over machines (patching, anti-malware etc) was ranked the highest the biggest security risk with regard to OT security (**28%**)

28%

- Potential operational disruption was considered the biggest consequence of failing to understand OT security risks (**26%**)

26%

- OT security will be either a medium or high priority for almost **70%** of participants' organisations over the next 12 months

70%

> **ALMOST 70% RESPONDENTS THOUGHT ICS ADVERSARIES POSED EITHER A MEDIUM OR HIGH TO ORGANISATIONS IN THE MIDDLE EAST.**

CHAPTER ONE

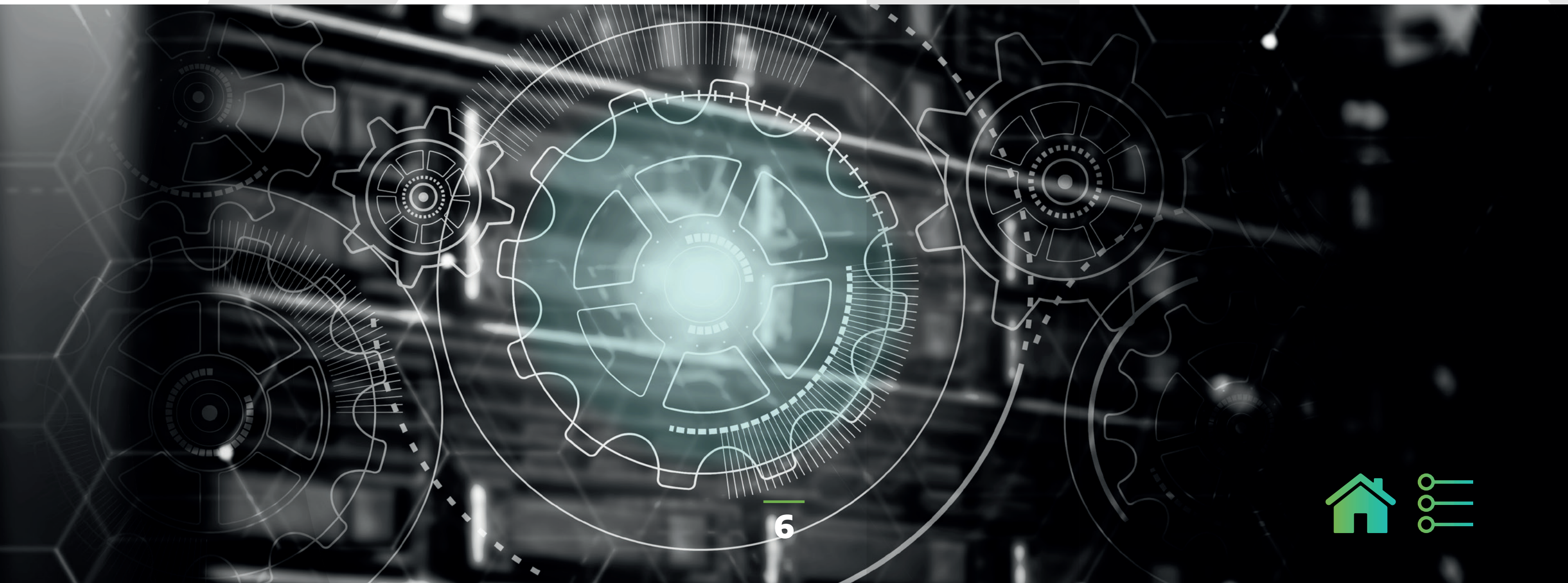
THE CHALLENGES AND THREAT LANDSCAPE

ENTERPRISE INFORMATION SECURITY has been a priority for many organisations for several years, but digitalisation of industrial environments triggered a need for change.

With ICS no longer neatly firewalled off from the rest of the network, attackers began to shift their focus. And while the impact of a major phishing attack or data theft incident can be devastating, an attack on critical systems can have a profound impact, potentially causing loss of life or compromising national security.

In this section, we explore how organisations are progressing their Digital Transformation strategies and the level of risk associated with ICS adversaries in the region.

> **WHILE THE IMPACT OF A MAJOR PHISHING ATTACK OR DATA THEFT INCIDENT CAN BE DEVASTATING, AN ATTACK ON CRITICAL SYSTEMS CAN HAVE A PROFOUND IMPACT.**

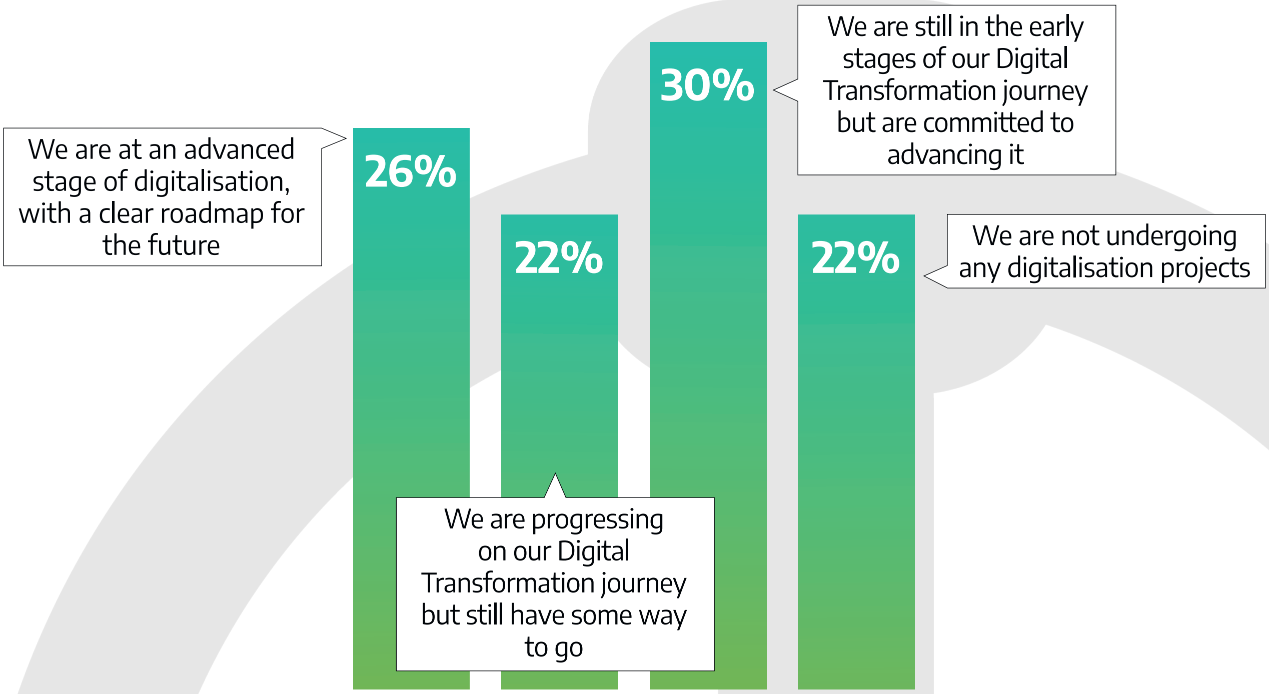


. . . CONTINUED

CHAPTER ONE

THE CHALLENGES AND THREAT LANDSCAPE

WHERE IS YOUR ORGANISATION CURRENTLY AT IN ITS DIGITAL TRANSFORMATION JOURNEY?



KEY TAKEAWAY

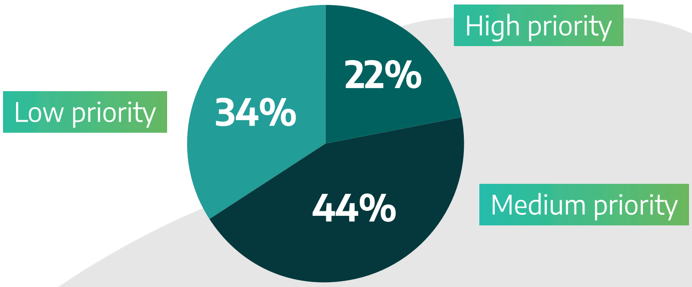
ALMOST 80% of respondents indicated their organisation was in the process of Digital Transformation. While some were at more advanced stages than others, this indicates the ongoing digitalisation of industrial environments – and the need to consider OT security as early as possible.

. . . CONTINUED

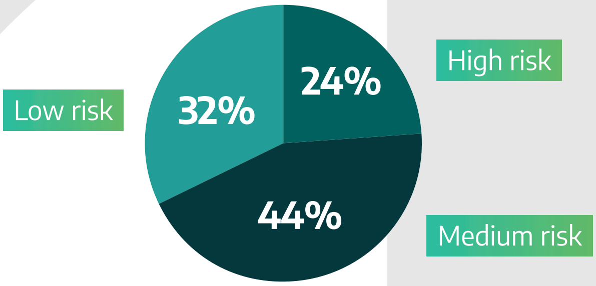
CHAPTER ONE

THE CHALLENGES AND THREAT LANDSCAPE

OVER THE LAST TWO YEARS, HOW HAS YOUR ORGANISATION PRIORITISED OT SECURITY?



HOW MUCH OF A RISK DO YOU THINK ICS ADVERSARIES POSE TO ORGANISATIONS IN THE MIDDLE EAST?



KEY TAKEAWAY

MORE THAN 65% of participants said their organisation had prioritised OT security in the last two years, while almost 70% said ICS adversaries posed a medium or high risk to organisations in the Middle East. This indicated the perceived level of threat and highlights a need to align this with future priorities.

. . . CONTINUED

CHAPTER ONE

THE CHALLENGES AND THREAT LANDSCAPE

ON A SCALE OF 1 TO 5 WHAT ARE YOUR BIGGEST SECURITY RISKS WITH REGARD TO OT SECURITY? RATE FROM 1 (MOST CHALLENGING) TO 5 (NOT SIGNIFICANT)

Top ranked	Second	Third
Management control over machines (patching, anti-malware etc) 28%	Human error (mistakes, lack of awareness) 28%	Human error (mistakes, lack of awareness) 24%
Malware (including ransomware) 24%	Nation state attacks 26%	Nation state attacks 20%
Unsecure networks 22%	Management control over machines (patching, anti-malware etc) 18%	Malware (including ransomware) 20%
Nation state attacks 20%	Unsecure network 14%	Management control over machines (patching, anti-malware etc) 18%
Human error (mistakes, lack of awareness) 6%	Malware (including ransomware) 14%	Unsecure networks 18%
OTHER (0)	OTHER (0)	OTHER (0)

KEY TAKEAWAY

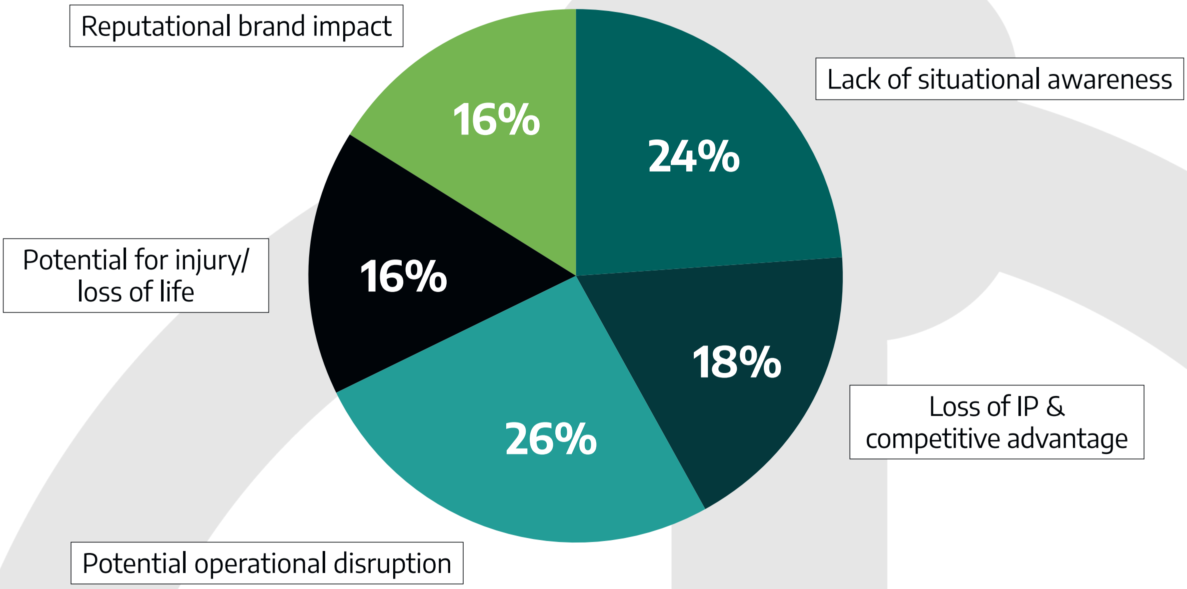
SIMILAR TO ENTERPRISE IT ENVIRONMENTS, some of the key risks to OT security were highlighted as ensuring patching and tools such as anti-malware were prioritised. Human error was also considered the second and third most challenging risk by participants. However, the highest ranked risks were split fairly evenly, illustrating the range of threats presented and the challenges organisations face.

. . . CONTINUED

CHAPTER ONE

THE CHALLENGES AND THREAT LANDSCAPE

WHAT, IN YOUR VIEW, IS THE BIGGEST CONSEQUENCE OF FAILING TO UNDERSTAND OT SECURITY RISKS?



KEY TAKEAWAY

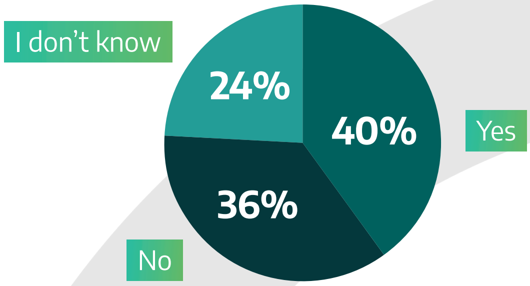
IN TRUTH, any one of these outcomes would be devastating for an organisation but the findings highlight how an attack on critical systems has the potential to cause operational disruption – and this impact was considered the biggest consequence of failing to understand OT security risks by participants.

CHAPTER TWO

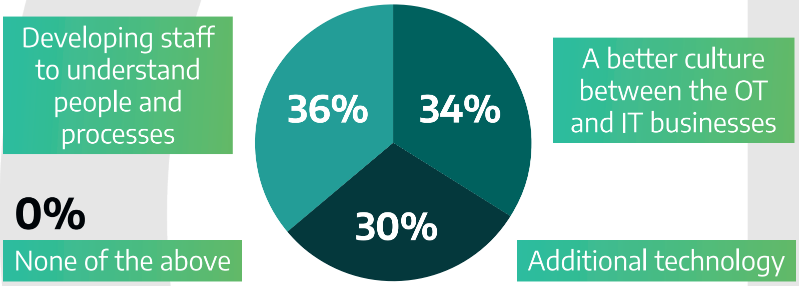
PRIORITIES AND PLANNING AHEAD

ASSET VISIBILITY is considered one of the key requirements to enabling cyber-resilience in critical infrastructure settings. After all, you can't protect what you don't know you have.

DO YOU CURRENTLY HAVE THE LEVEL OF ASSET VISIBILITY OVER OT DEVICES THAT YOU REQUIRE?



WHICH OF THE FOLLOWING THREE DO YOU THINK IS MOST IMPORTANT WHEN IT COMES TO OBTAINING BETTER VISIBILITY OF YOUR OT STACK?



KEY TAKEAWAY

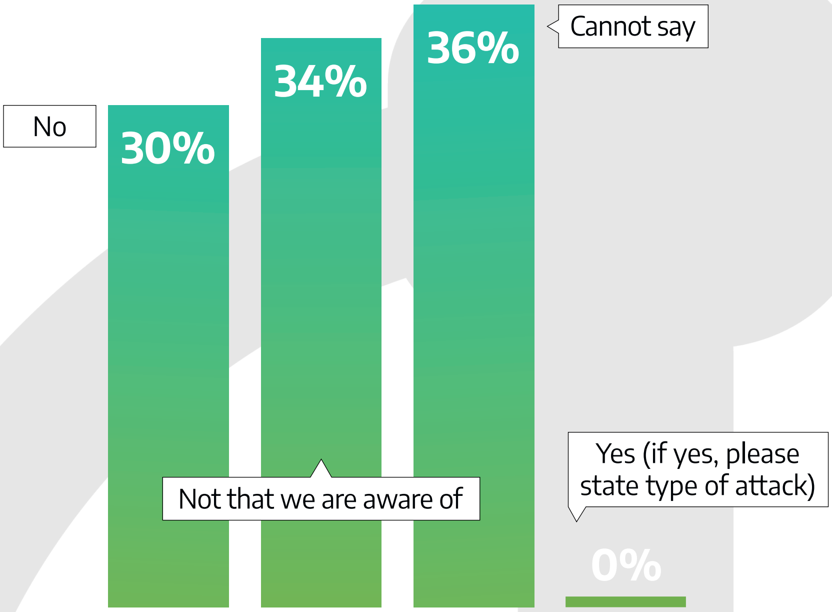
WHILE 40% of participants said their organisation had the required level of asset visibility, 60% said they either did not, or did not know. This highlights that there is some way to go to ensuring visibility – one of the most important elements when it comes to protecting against threats. Investing in training to develop staff to better understand people and processes was considered the most important way of enabling this, according to survey participants.

. . . CONTINUED

CHAPTER TWO

PRIORITIES AND PLANNING AHEAD

HAS YOUR ORGANISATION EXPERIENCED A SECURITY INCIDENT IMPACTING YOUR OT STACK DURING THE LAST 12 MONTHS?

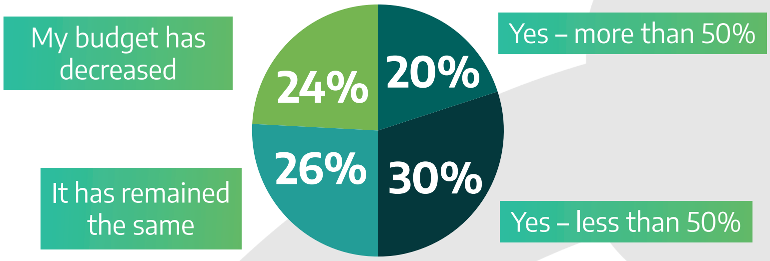


. . . CONTINUED

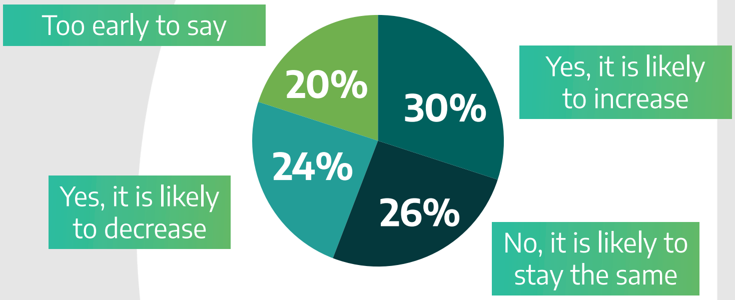
CHAPTER TWO

PRIORITIES AND PLANNING AHEAD

HAS YOUR OT SECURITY BUDGET BEEN ADJUSTED DUE TO INCREASED AWARENESS OF THE RISKS IN THE LAST 12 MONTHS?



IS YOUR OT SECURITY BUDGET LIKELY TO BE ADJUSTED IN THE NEXT 12 MONTHS?



KEY TAKEAWAY

INCREASED INVESTMENT in OT security will be critical for shoring up defences and the findings highlight organisations are taking this seriously, with 50% of respondents stating OT security budgets had been adjusted within the last 12 months and 30% stating this would likely be adjusted further in the next 12.

. . . CONTINUED

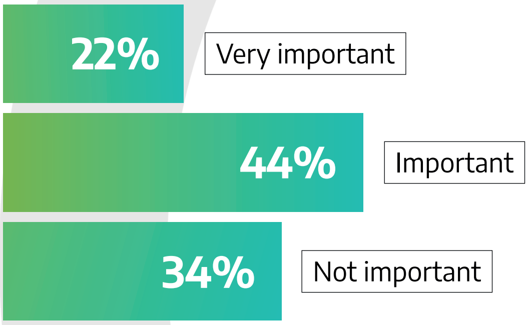
CHAPTER TWO

PRIORITIES AND PLANNING AHEAD

WHAT DO YOU LOOK FOR WHEN ASSESSING WHICH VENDOR TO WORK WITH ON OT SECURITY PROJECTS? (RANK FROM 1) MOST IMPORTANT TO 5) LEAST IMPORTANT)

Top	Second	Third
Communication 34%	Cost 24%	Useability of product 30%
A recommendation from someone else (word of mouth) 22%	Analyst reports 22%	Analyst reports 28%
Cost 20%	Useability of product 22%	Communication 16%
Analyst reports 18%	Communication 20%	A recommendation from someone else (word of mouth) 14%
Useability of product 6%	A recommendation from someone else (word of mouth) 12%	Cost 12%

HOW IMPORTANT ARE LOCAL PARTNERS FOR YOU WHEN ASSESSING A SECURITY VENDOR?



KEY TAKEAWAY

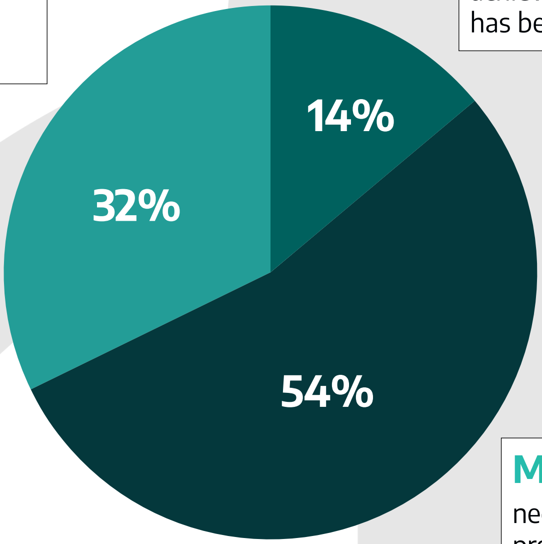
A LEADING PROVIDER of OT security protection will be a key partner for organisations. Respondents highlighted the importance of good communication from vendors, alongside a recommendation from someone else. Cost and product useability were ranked as second and third most important aspects, while 66% of respondents highlighted that local partners were either important or very important.

. . . CONTINUED

CHAPTER TWO

PRIORITIES AND PLANNING AHEAD

LOOKING AHEAD OVER THE NEXT 12 MONTHS, HOW MUCH OF A PRIORITY WILL OT SECURITY BE FOR YOUR ORGANISATION?



HIGH PRIORITY. We now have many more connected devices and therefore many more risks – achieving a high level of OT security has become a strategic objective.

LOW PRIORITY. We are not prioritising OT security.

MEDIUM PRIORITY. We need to take steps to become better protected against the increased risks, but we must balance this against other security objectives.

KEY TAKEAWAY

AS DIGITALISATION CONTINUES, attackers will continue to find new ways to target industrial control systems. Thankfully, a majority of respondents stated that OT security will either be a medium or high priority for their organisation over the next 12 months, highlighting the importance of defining OT security strategies and investments.

CONCLUSION

WITH A MAJORITY of participants indicating that their organisation was undertaking digitalisation – and 55% not yet at an advanced stage – there is no better time to build in OT security strategies to ensure protection and resiliency during an exciting time of transformation.

The consequences of OT attacks can be catastrophic – survey respondents were particularly concerned about operational disruption – and sophisticated threat groups are constantly researching and carrying out reconnaissance to prepare themselves for the day that they cross the divide.

This level of sophistication can take several years to achieve, so it's important that organisations understand the need to look ahead and focus on long-term strategies for cyber protection.

Thankfully, the findings highlight that spend on OT security has increased in line with awareness of threats, with many survey participants expecting budgets to increase further over the next 12 months.

By taking a long-term approach and securing a trusted partner to help obtain crucial asset visibility and provide threat intelligence, organisations can put themselves on the path to improved cyber-resilience and ensure critical systems are not impacted.

> **THIS LEVEL OF SOPHISTICATION CAN TAKE SEVERAL YEARS TO ACHIEVE, SO IT'S IMPORTANT THAT ORGANISATIONS UNDERSTAND THE NEED TO LOOK AHEAD AND FOCUS ON LONG-TERM STRATEGIES FOR CYBER PROTECTION.**

DRAGOS

CxO priorities

A Lynchpin Media BRAND

FIND OUT MORE

Sponsored by

DRAGOS

Innovations Hub Building 2,
Al Falak Street, Unit B104,
Dubai Internet City

www.dragos.com

CxO priorities

CxO Priorities, a Lynchpin Media Brand
63/66 Hatton Garden
London, EC1N 8LE

www.cxopriorities.com