CYBER SECURITY

as a Business Differentiator in Healthcare

Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

AGENDA

CYBER SECURITY
as a Business Differentiator in Healthcare

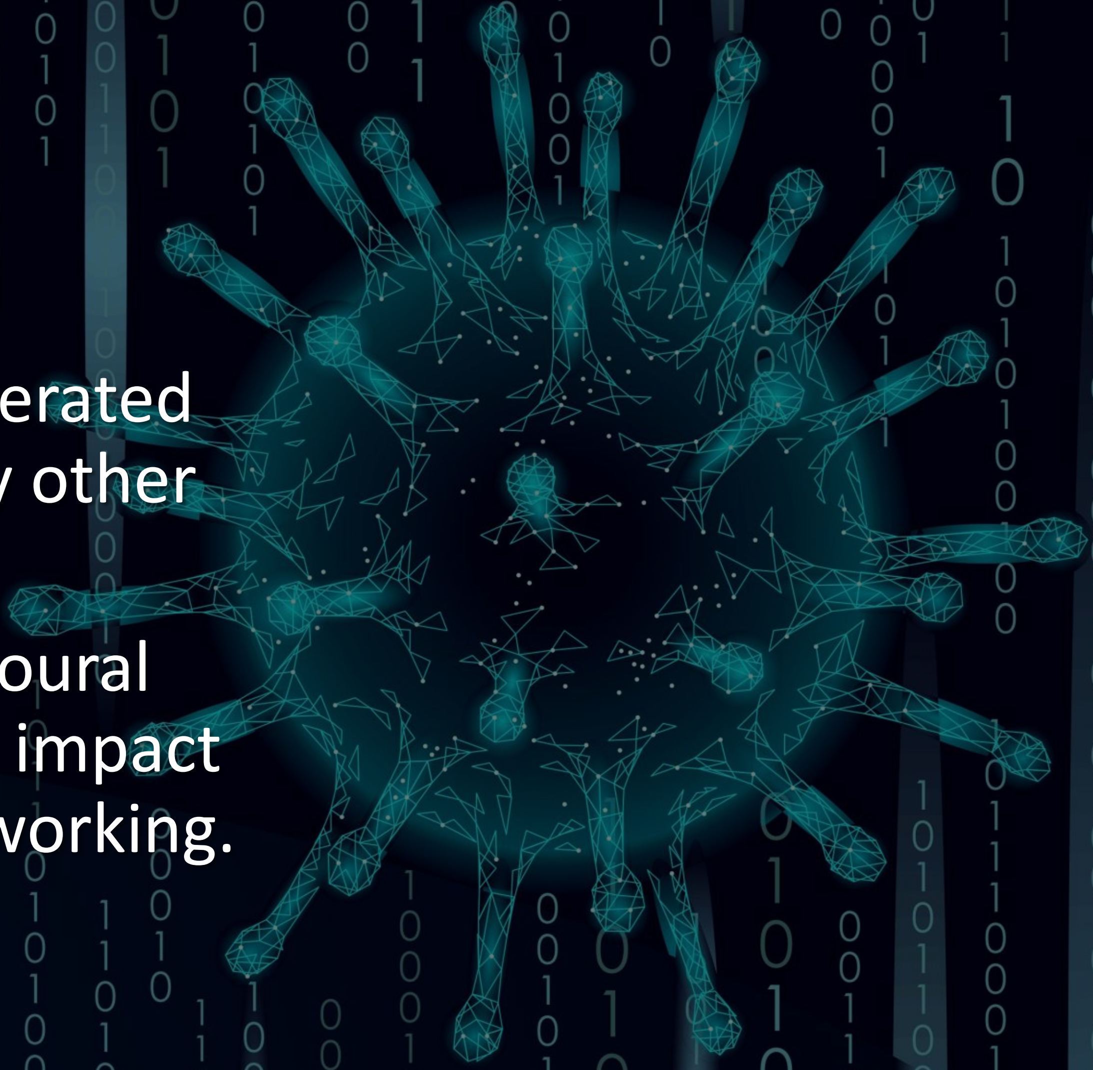
1. INTRODUCTION
2. THREAT LANDSCAPE
3. HEALTHCARE CHALLENGES
4. TRANSFORMING HEALTHCARE
5. REGULATORY COMPLIANCE
6. MEDICAL TECHNOLOGY
7. THIRD-PARTY RISK MANAGEMENT

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

INTRODUCTION

> The coronavirus has accelerated digitisation more than any other previous driver.
>
> Some of the new behavioural patterns will have a lasting impact on our society and way of working.



Crown Commercial Service *Supplier*

ABOUT US

Supporting Digital Transformation and Driving Better Value

Medicare Network is a niche, forward-thinking Cyber Security and Risk Management company dedicated to supporting and solving healthcare providers and pharmaceutical organisations cyber security challenges.

We are a vendor agnostic company that carefully identifies and selects the latest next-generation solutions that leverage the latest cloud, AI and machine learning capabilities, to intelligently detect, identify and respond to any potential cyber threats to Information Technology, Operational Technology and Medical Technology environments.

Medicare **Network**
More intelligent, More Secure

THREAT LANDSCAPE

> This invisible enemy which transcends geography, languages and political borders is responsible for approximately $3 trillion worth of commercial losses in 2015 and is forecasted to impact the global society to the tune of $6 trillion in 2021.

Source: The Data Privacy Group

CYBER THREATS

Cybercriminals are Always Evolving

Healthcare data is highly sensitive and very valuable, as recently as May 5, 2020 the UK's National Cyber Security Centre (NCSC) issued an alert to warn that ‘**advanced persistent threat (APT) groups are exploiting the Covid-19 pandemic**’ to specifically target ‘**healthcare bodies and pharmaceutical companies**’.

Patient’s safety could be put at risk.

Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

CYBER THREATS

Organisations Behind Cybercrime

INTEREST

STATE-SPONSORED	HACKTIVIST	CRIMINAL
Intellectual property	Sensationalism	Monetisation
Information	Disruption	Data value
Disruption	Environmentalism	Intellectual property
Warfare	Social impact	Financially motivated

CYBER RESILIENCE IN HEALTHCARE

Threat Landscape

- In February 2018 the Department of Health and Social Care published ‘Securing cyber resilience in health and care: which set out the actions taken by the Department and its Arm’s-Length Bodies to improve the cyber security of the health and care system both before and after the May 2017 WannaCry cyber attack.
- This document provides a further update on progress and development of future plans to improve cyber resilience within the NHS.

Source: Department of Health and Social Care

Department of Health & Social Care

Securing cyber resilience in health and care

Progress update October 2018

October 2018

NHS England

of the

February 2018

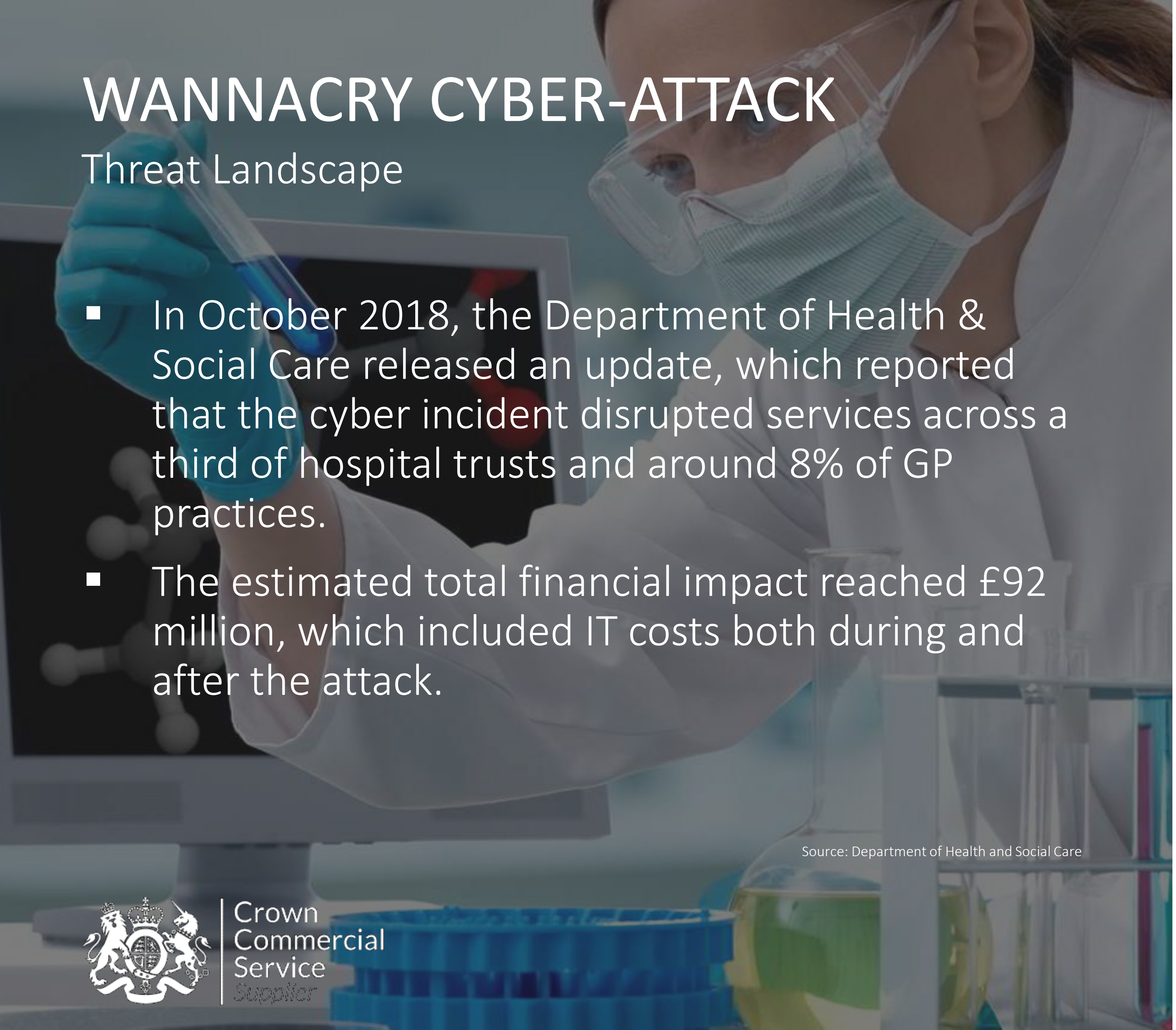
Crown Commercial Service Supplier

Medicare Network

More intelligent, More Secure

WANNACRY CYBER-ATTACK

Threat Landscape



- In October 2018, the Department of Health & Social Care released an update, which reported that the cyber incident disrupted services across a third of hospital trusts and around 8% of GP practices.
- The estimated total financial impact reached £92 million, which included IT costs both during and after the attack.

Source: Department of Health and Social Care

Department of Health & Social Care

Securi
health
Progress

Department of Health & Social Care

NHS Improvement

NHS England

Lessons learned review of the WannaCry Ransomware Cyber Attack

February 2018

Crown Commercial Service Supplier

Medicare Network
More intelligent, More Secure

DID YOU KNOW?

Cybercrime in Healthcare

Crown Commercial Service Supplier

A medical record fetches

8 to 10 times

the price of a credit card on the black market

92%

of all healthcare providers reported at least one data breach in the last two years

Source: Cisco Systems, Inc

Medicare Network

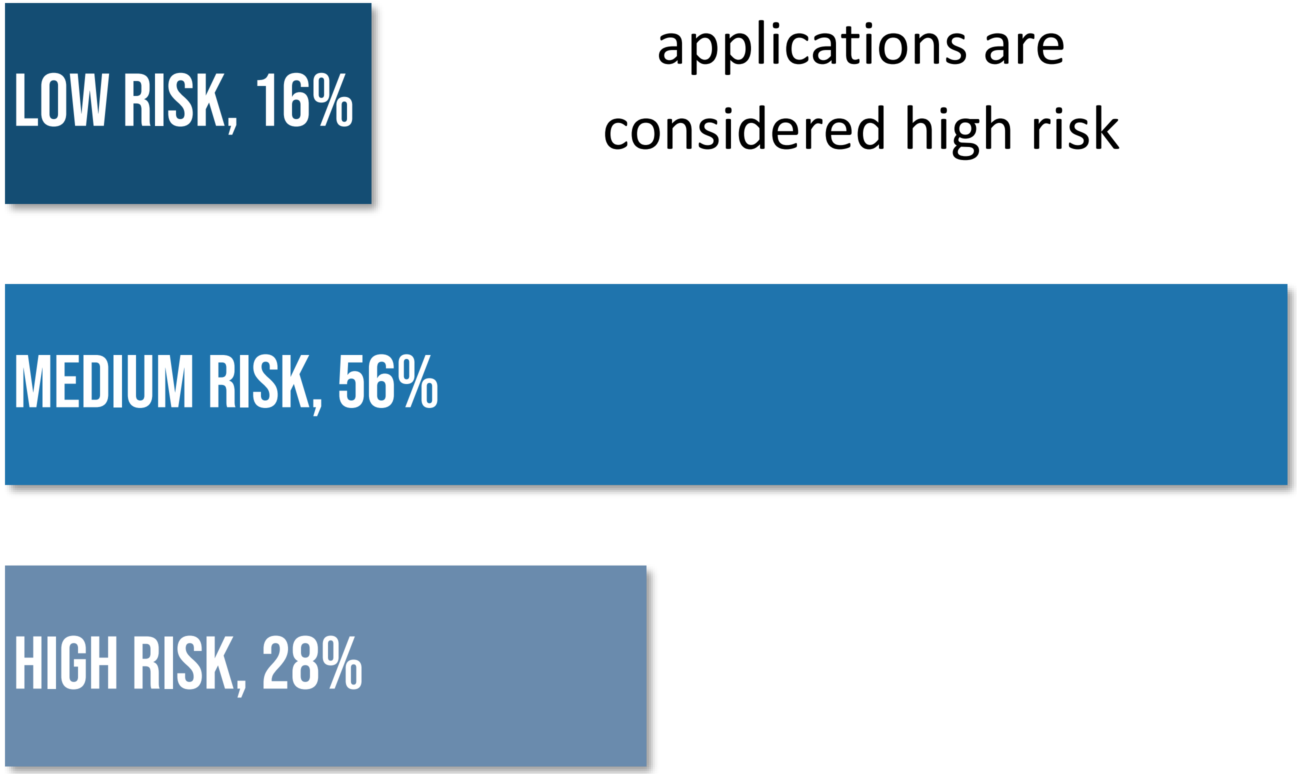
More intelligent, More Secure

DID YOU KNOW?

Threats to Healthcare

Compared to all industries, **healthcare and pharmaceuticals** have some of the least mature cyber security operations.

28% of all healthcare applications are considered high risk



Source: Cisco Systems, Inc

Crown Commercial Service Supplier

Medicare Network
More intelligent, More Secure

HEALTHCARE CHALLENGES

> Many public sector organisations are starting to initiate digital transformation programmes. It is imperative to ensure that such changes implement a security-by-design approach, rather than bolting on or retro-fitting security.

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

THE ERA OF DIGITAL CONVERGENCE

The World is Converging for Healthcare

Digital convergence is a certainty of the future. Technology aided healthcare comes with its own set of unique challenges, most prominent being regulatory implications and security threats.

Probably more than any other industry, healthcare see immediate and tangible benefits of digital convergence as health workers are able to deal with patients much faster and more efficiently.

Separate enterprise IT and OT means there may be duplication in technology investments and staff. Consolidating both can deliver sizeable Capex and Opex savings.

Many devices such as Medical Technology are not built with the same security in mind. Visibility and management needs to be considered as does interoperability.

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

Crown
Commercial
Service
Supplier

DIGITALISATION JOURNEY

Observations on Digitalisation in Healthcare

One of the greatest challenges faced in creating a highly digitised organisation, whilst holistically securing systems and safeguarding patient's data.

Many healthcare providers still adopt a very reactive approach towards cyber security or retrospectively 'plug' perceived gaps in planning.

Cyber security needs to be considered at the planning stage, along with a comprehensive cyber security awareness, education, and training program.

Cyber security is a way to ward off cyber-attacks and should be part of ongoing and constant review and testing regimes, additionally aligned to compliance and contractual obligations.

Medicare Network
More intelligent, More Secure

SECURITY TRANSFORMATION

Cyber Security to Support your Strategic Goals

There is still more to be done in terms of building effective C-level relationships, support and commitment.

Few industries have this level of critical and sensitive personal information that is collected, processed and stored.

Current security models are reactive, with new controls bolted or retro fitted onto insecure legacy architecture.

Security needs to be viewed as part of the business, not just a cog in the IT wheel.

Crown
Commercial
Service
Supplier

SECURITY CHALLENGES

Cyber Security Myths

WE CONDUCTED PENETRATION TESTING

Security testing should cover the entire infrastructure so that the company can quickly remediate / mitigate all identified vulnerabilities.

WE'VE NEVER BEEN ATTACKED SO OUR SECURITY SYSTEM MUST BE GOOD

Caution: threats continue to grow and become more advance and complex.

WE'VE DESIGNED HIGH-END SECURITY TOOLS

Security tools are only effective when properly configured, integrated and controlled within all security operations.

WE COMPLY WITH INDUSTRY REGULATIONS AND BEST PRACTICES

Compliance requirements often only meet the minimum safety measures and not all critical systems and information.

A THIRD-PARTY PROVIDER RUNS OUR SECURITY

Regardless of the competence and capabilities of the provider, the question is whether complex threats in a company will be taken seriously enough for a third party to sufficiently protect it.

WE'VE INVESTED IN STRICT SECURITY CONTROLS

It is not enough to rely on standard IT security controls alone. Critical business services should be above all protected.

OUR SECURITY IS MANAGED ADEQUATELY BY THE IT TEAM

A threat can take over an entire business. Therefore, management should work closely with IT and OT teams.

WE ONLY NEED TO SECURE OUR INTERNET APPLICATIONS

One should also be equipped against internal threats and member / staff abuse.

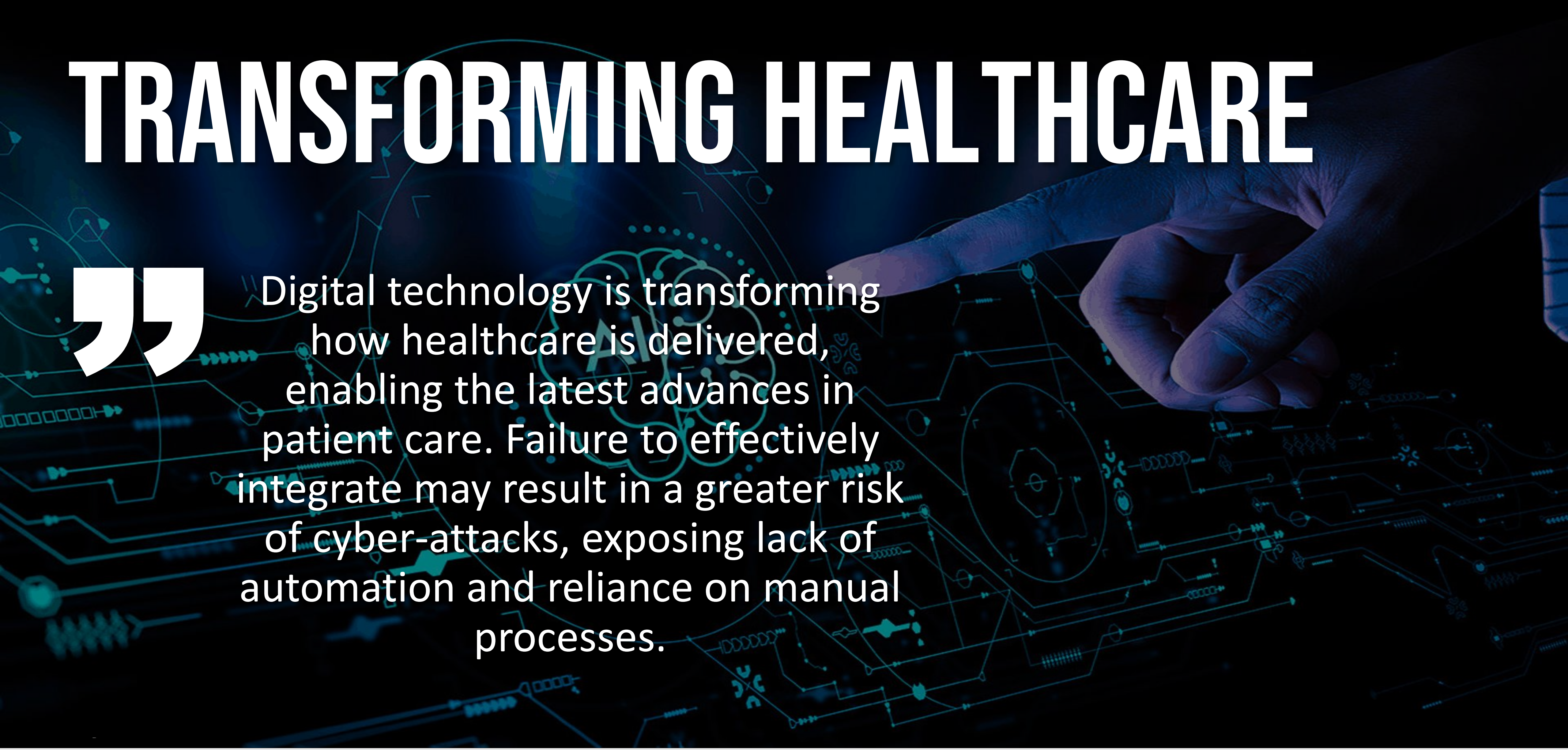
WE'VE COMPLETED OUR SECURITY PROJECT

Security is an ongoing project that will never be completed.

WE AREN'T STATISTICALLY AT RISK

Every company is at risk from a compromise or data breach and should be prepared.

TRANSFORMING HEALTHCARE



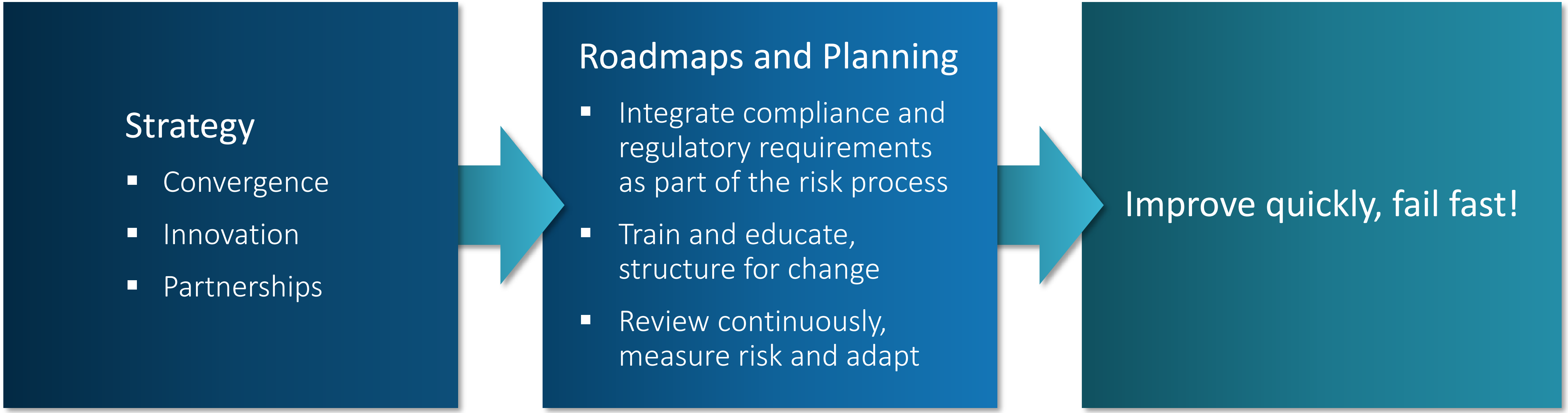
> Digital technology is transforming how healthcare is delivered, enabling the latest advances in patient care. Failure to effectively integrate may result in a greater risk of cyber-attacks, exposing lack of automation and reliance on manual processes.

Crown Commercial Service Supplier

Medicare Network
More intelligent, More Secure

DIGITAL TRANSFORMATION APPROACH

Build Trust and Resilience



Strategy

- Convergence
- Innovation
- Partnerships

Roadmaps and Planning

- Integrate compliance and regulatory requirements as part of the risk process
- Train and educate, structure for change
- Review continuously, measure risk and adapt

Improve quickly, fail fast!

Crown Commercial Service Supplier
Medicare Network
More intelligent, More Secure

STRATEGIC TRANSFORMATION PATHS

Building Future Capabilities

Treat cyber security as a digital transformation enabler to build future capabilities to rapidly reduce cyber risks and adopt innovative cyber solutions that support your strategic goals.

Invest to strengthen fundamentals, including people making cyber security part of the organisation’s culture enabling compliance and regulatory commitments under GDPR and NIS.

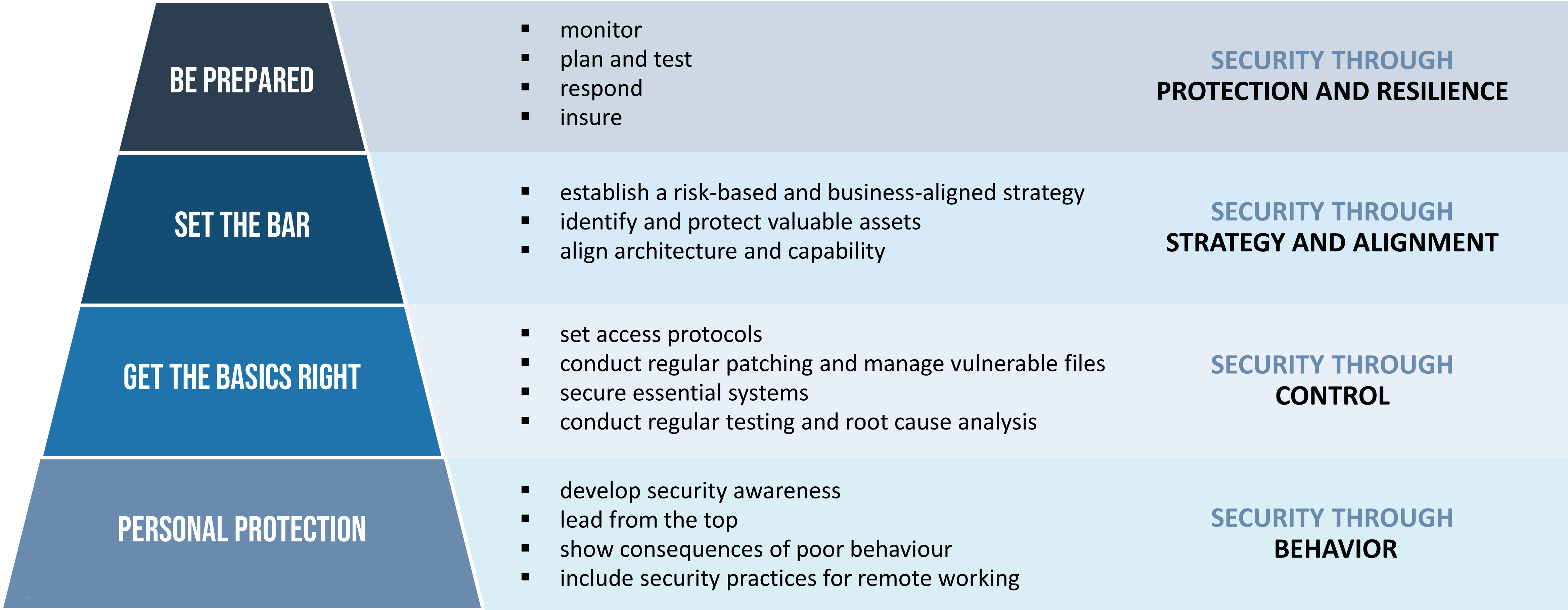
Perform regular security testing to assess and review increasing threats. Serving to protect your organisation as well as responding to regulators requirements for continuous and consistent testing.

Adopt innovation, leveraging cloud as a platform, use of integrated security tools, tapping into AI and machine learning automation to improve efficient and cost effectiveness.

Medicare Network
More intelligent, More Secure

IMPROVE SECURITY POSTURE

Transforming Cyber Security in Healthcare



BE PREPARED

- monitor
- plan and test
- respond
- insure

SECURITY THROUGH
PROTECTION AND RESILIENCE

SET THE BAR

- establish a risk-based and business-aligned strategy
- identify and protect valuable assets
- align architecture and capability

SECURITY THROUGH
STRATEGY AND ALIGNMENT

GET THE BASICS RIGHT

- set access protocols
- conduct regular patching and manage vulnerable files
- secure essential systems
- conduct regular testing and root cause analysis

SECURITY THROUGH
CONTROL

PERSONAL PROTECTION

- develop security awareness
- lead from the top
- show consequences of poor behaviour
- include security practices for remote working

SECURITY THROUGH
BEHAVIOR

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

DEVELOPING SECURITY

Cyber Security Focus with People

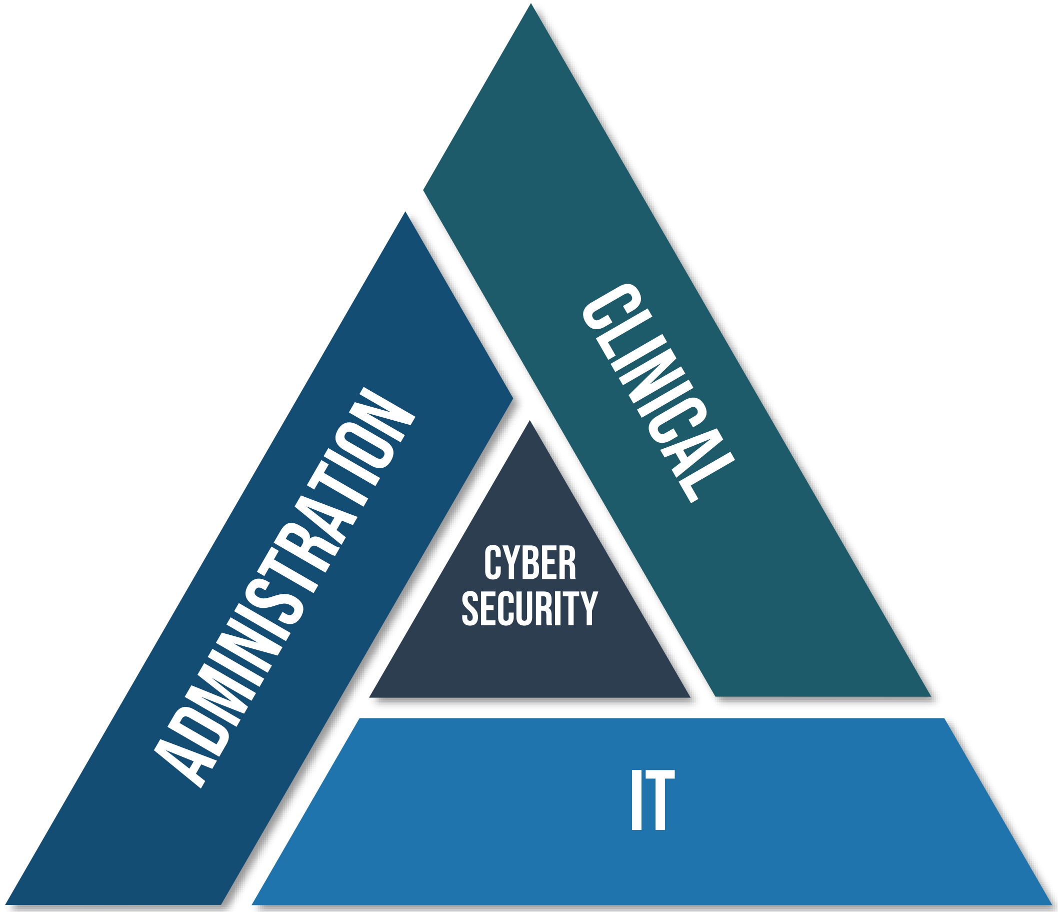
Building Unified Teams

- All business units must work together toward a unified security strategy.
- Make cybersecurity a differentiator for healthcare with an enterprise-wide decision to make it a priority.

Educating Employees

- Despite the sophisticated technologies available, many attacks can be traced back to relatively simple tactics such as phishing attacks and social engineering.
- Many security experts say that employees pose the biggest cyber security risk to an organisation.

Crown Commercial Service Supplier



CLINICAL

ADMINISTRATION

CYBER SECURITY

IT

Medicare Network

More intelligent, More Secure

ENHANCING SECURITY

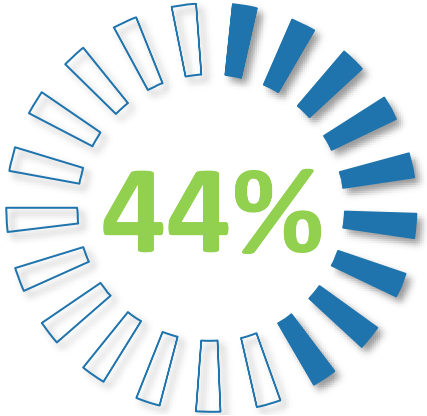
Cyber Security Working with Technology

Integrate Security Technology

- Now is the time for healthcare providers to streamline their security tools and identify next-generation enterprise-wide solutions.
- Integrate third-party tools to maximize prior investments, minimise duplication and save money.

Incorporate More Automation

- The lack of automation and reliance upon manual risk management processes makes it difficult to keep pace with cyber threats.
- Automated technologies helps to identify and target real threats to reduce the impact or while containing the spread of malware.



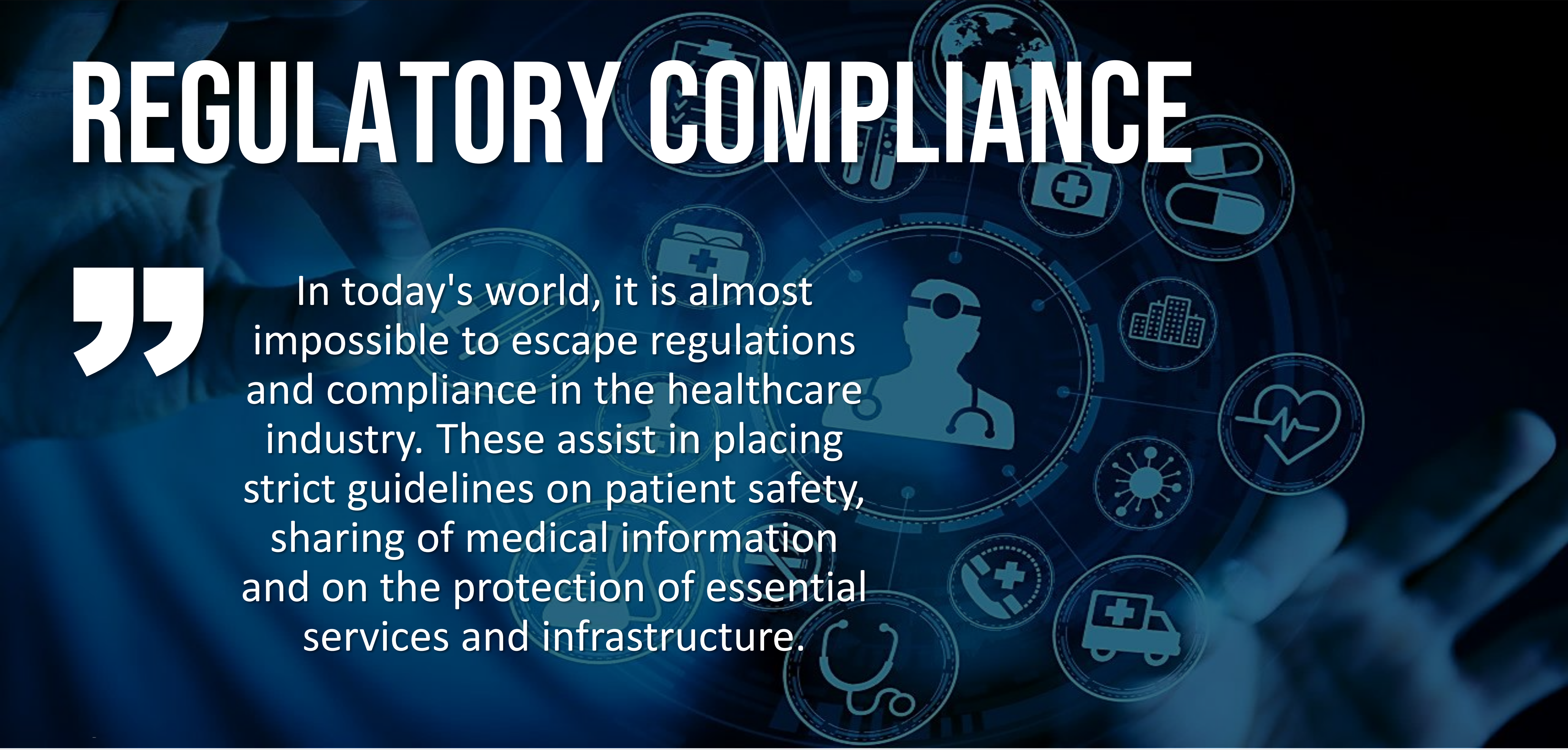
of security alerts are never investigated

Source: Cisco Systems, Inc

Crown Commercial Service Supplier

Medicare Network
More intelligent, More Secure

REGULATORY COMPLIANCE



> In today's world, it is almost impossible to escape regulations and compliance in the healthcare industry. These assist in placing strict guidelines on patient safety, sharing of medical information and on the protection of essential services and infrastructure.

Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

REGULATORY COMPLIANCE

Automating Compliance and Reducing Policy Breaches

The General Data Protection Regulation (GDPR), failure to comply can result in huge fines of up to €20 million or 4% of global annual revenue.

The Security of Network and Information Systems (NIS), ensures that operators of essential services have acceptable cyber security measures in place, failure resulting in fines as much as £17 million.

Data Security and Protection Toolkit (DSPT), supports **NHS Trusts and Foundation Trusts** to meet the requirements of the above legislations.

Medicines and Healthcare products Regulatory Agency (MHRA), will take on the responsibilities for the UK medical devices market from 1 January 2021, which is currently undertaken through the EU system.

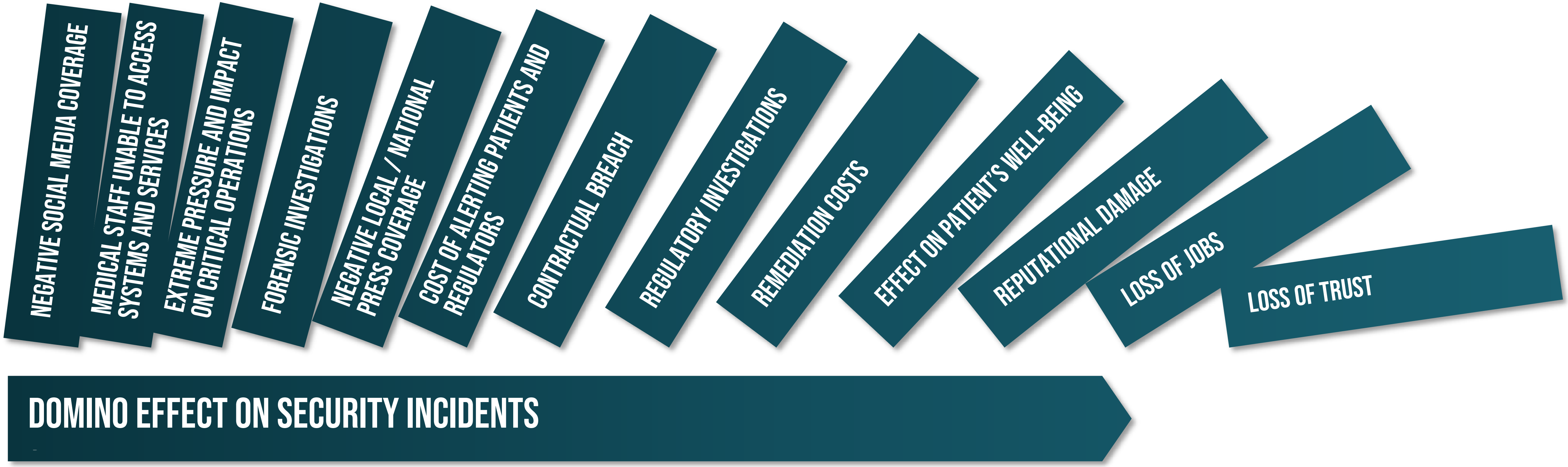
Crown
Commercial
Service
Supplier

PROTOCOL
INITIALIZATI
e process /// fixing /// password XXXX XXX XXXX XXXXX
one /// final pass /// password denied
----------- stop
EMONSTRATION 0001 .... finished
EMONSTRATION 0002 .... progress MMN 000xxx00000xx

Medicare
Network
More intelligent, More Secure

CYBER SECURITY IMPACTS

Domino Effect on Security Incidents



NEGATIVE SOCIAL MEDIA COVERAGE

MEDICAL STAFF UNABLE TO ACCESS SYSTEMS AND SERVICES

EXTREME PRESSURE AND IMPACT ON CRITICAL OPERATIONS

FORENSIC INVESTIGATIONS

NEGATIVE LOCAL / NATIONAL PRESS COVERAGE

COST OF ALERTING PATIENTS AND REGULATORS

CONTRACTUAL BREACH

REGULATORY INVESTIGATIONS

REMEDIATION COSTS

EFFECT ON PATIENT'S WELL-BEING

REPUTATIONAL DAMAGE

LOSS OF JOBS

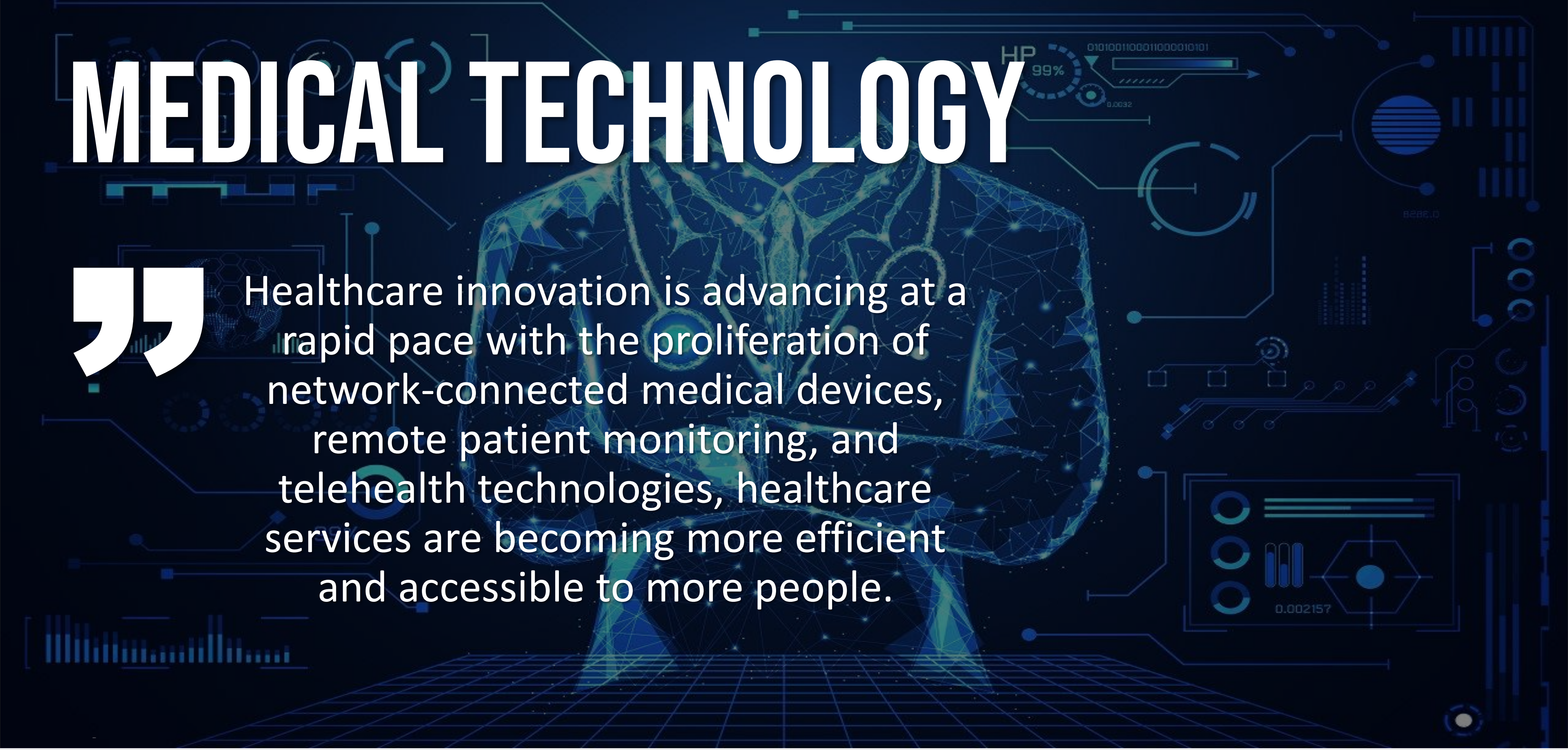
LOSS OF TRUST

DOMINO EFFECT ON SECURITY INCIDENTS

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

MEDICAL TECHNOLOGY



> Healthcare innovation is advancing at a rapid pace with the proliferation of network-connected medical devices, remote patient monitoring, and telehealth technologies, healthcare services are becoming more efficient and accessible to more people.

Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

MEDICAL DEVICE RISK EXPOSURE

Healthcare's Expanding Risk Landscape

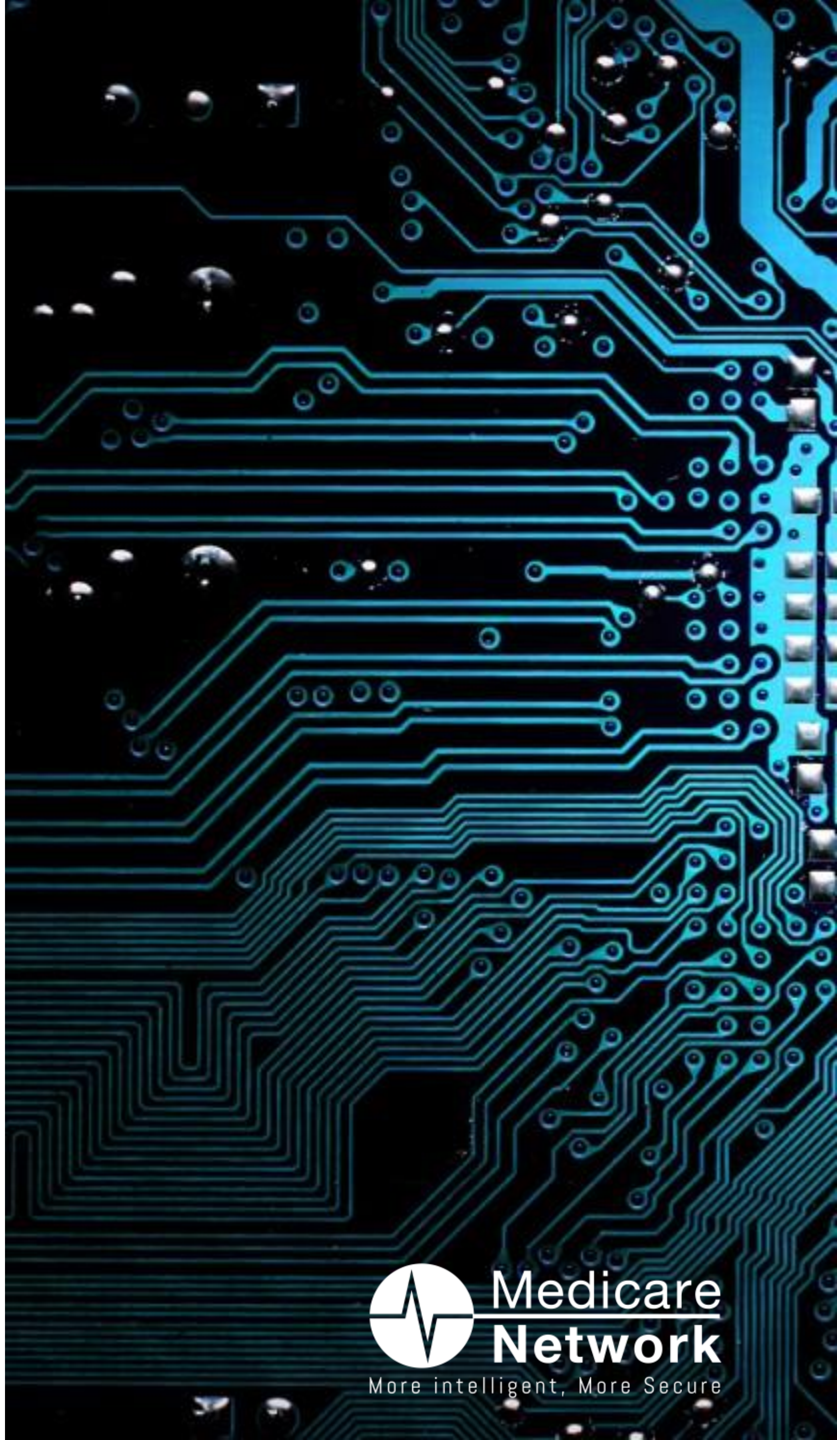
Healthcare providers use connected medical devices to provide better patient outcomes by capturing more precise data and closely monitoring patient conditions.

Components of these devices and the links between them have become targets for cyber-attacks, threatening patient well-being and loss of service.

This risk is especially high in the healthcare sector where the health of individuals may be in danger and where interruptions in service or operation could cause loss of life.

In a recent alert the U.S. Department of Homeland Security highlighted risks affecting 300 medical devices, including drug infusion pumps, ventilators and external defibrillators.

Crown
Commercial
Service
Supplier



Medicare
Network
More intelligent, More Secure

MEDICAL DEVICES

Threat Landscape to Medical Technology

Connected medical devices can make up 74% of the devices on a hospital’s network.

Source: Forrester New Wave

Several cases have been identified over the past few years where attackers directly compromised medical devices as part of overall campaigns against hospitals.

Inevitably, the risk is only going to increase as more connected medical devices are deployed within a clinical environment.

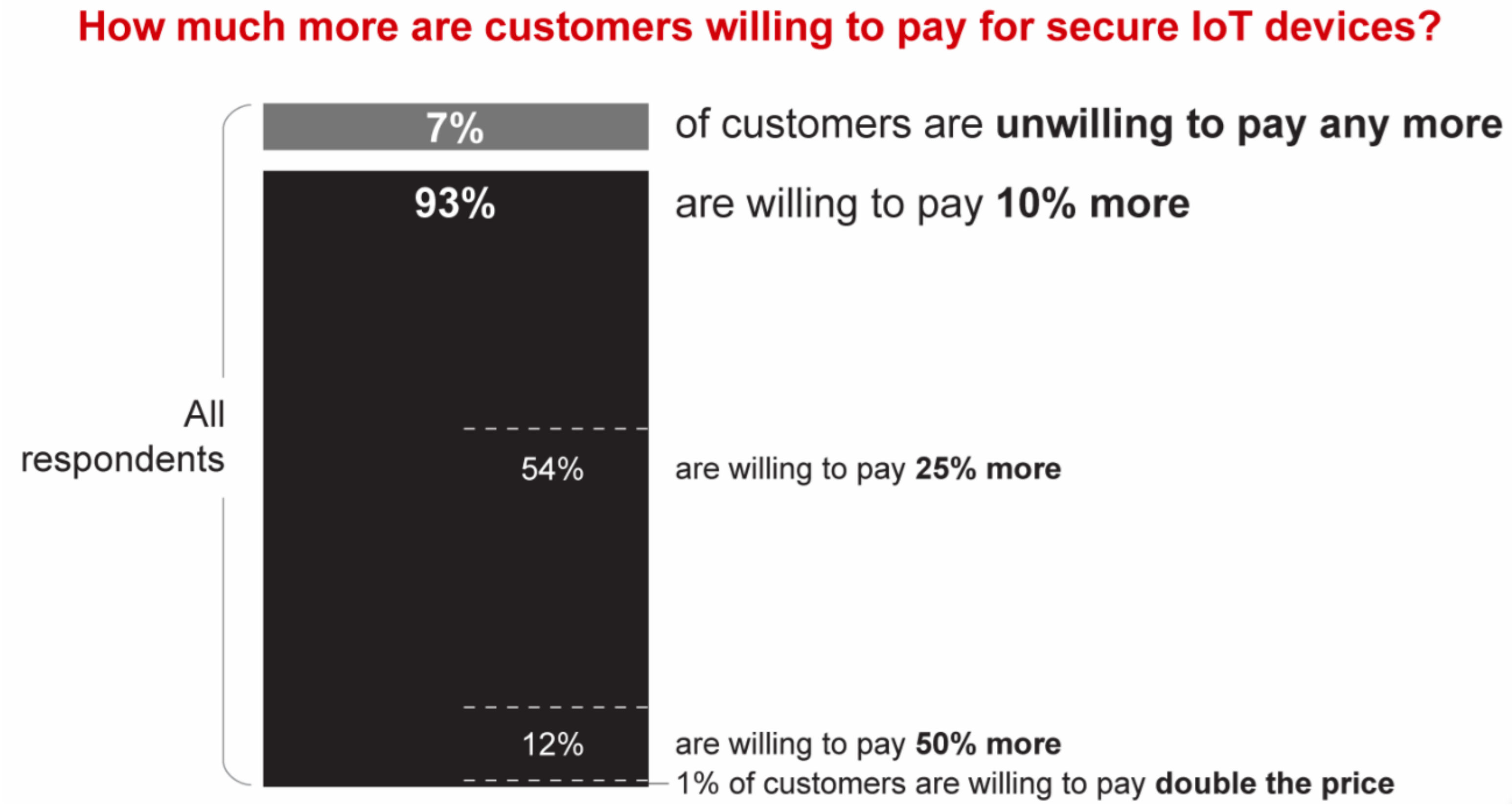
Crown Commercial Service Supplier

Medicare Network
More intelligent, More Secure

HEALTHCARE NEEDS TO INVEST

Budget for Security in Medical Devices

How much more are customers willing to pay for secure IoT devices?



7% of customers are **unwilling to pay any more**

93% are willing to pay **10% more**

54% are willing to pay **25% more**

12% are willing to pay **50% more**

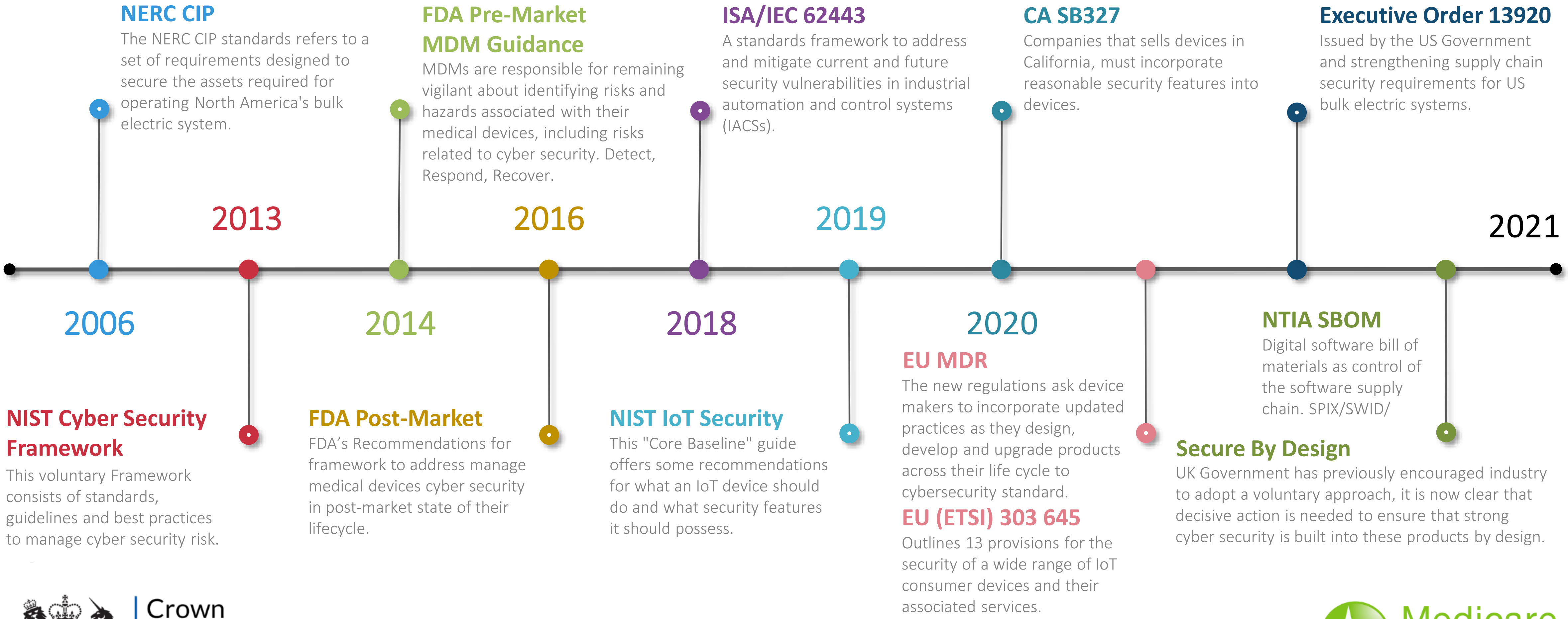
1% of customers are willing to pay **double the price**

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

CONNECTED DEVICE REGULATIONS

Market Dynamics



2006

NERC CIP

The NERC CIP standards refers to a set of requirements designed to secure the assets required for operating North America's bulk electric system.

2013

NIST Cyber Security Framework

This voluntary Framework consists of standards, guidelines and best practices to manage cyber security risk.

2014

FDA Pre-Market MDM Guidance

MDMs are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cyber security. Detect, Respond, Recover.

2016

FDA Post-Market

FDA's Recommendations for framework to address manage medical devices cyber security in post-market state of their lifecycle.

2018

ISA/IEC 62443

A standards framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).

2019

NIST IoT Security

This "Core Baseline" guide offers some recommendations for what an IoT device should do and what security features it should possess.

2020

CA SB327

Companies that sells devices in California, must incorporate reasonable security features into devices.

EU MDR

The new regulations ask device makers to incorporate updated practices as they design, develop and upgrade products across their life cycle to cybersecurity standard.

EU (ETSI) 303 645

Outlines 13 provisions for the security of a wide range of IoT consumer devices and their associated services.

Executive Order 13920

Issued by the US Government and strengthening supply chain security requirements for US bulk electric systems.

NTIA SBOM

Digital software bill of materials as control of the software supply chain. SPIX/SWID/

Secure By Design

UK Government has previously encouraged industry to adopt a voluntary approach, it is now clear that decisive action is needed to ensure that strong cyber security is built into these products by design.

2021

Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

INTERNET OF MEDICAL THINGS

Key Security Requirements

Security by Design

- Hardware security
- Device identity and cryptography
- SBOM Transparency of the software supply chain
- VEX, VPT Continuous security gap assessment

Built into Operation

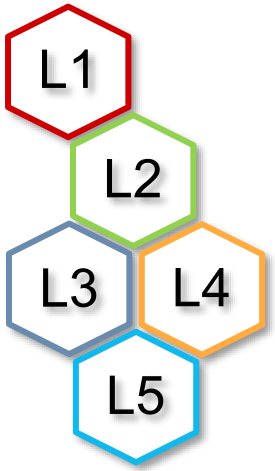
- Incident Response (EDR) HIDS, SIEM and IPS
- Firmware Lifecycle Management
- Patient Present / Tamper Detection
- Privileged Access Management

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

INTERNET OF MEDICAL THINGS

The Need for Software Bill of Materials



- Software is combination of smaller building blocks libraries.
- When vulnerability discovered in one of these blocks it becomes a major source of risk in modern software.
- Can any healthcare organisation that makes or uses IoMT devices answer a simple question.

HOW VULNERABLE ARE OUR MEDICAL DEVICES?

SCALING VULNERABILITIES

Vulnerability Prioritisation Technology is Key

500 vulnerabilities identified in the risk assessment report. How do we classify and prioritise the highest impacting vulnerabilities?

How do we address the most critical vulnerabilities when we do not have the time or resources to review and mitigate all of the findings!

How do we focus our efforts only on the highly exploitable vulnerabilities and the highest impacting on our medical devices’ security position?

How do we repeat and remediate for every medical device without affecting our performance or interrupting the organisations' operations?

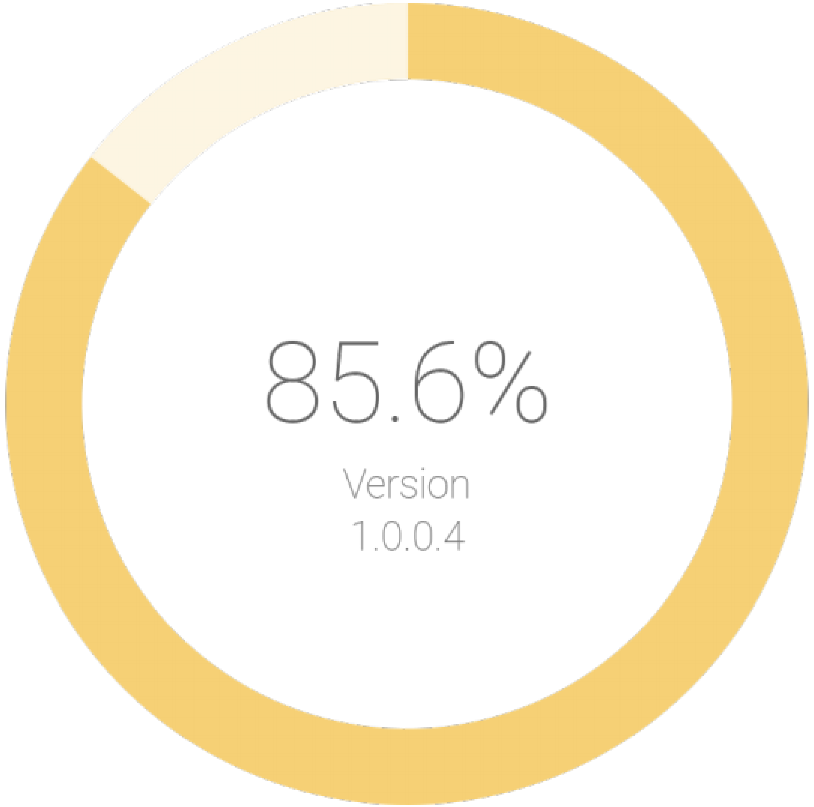
Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

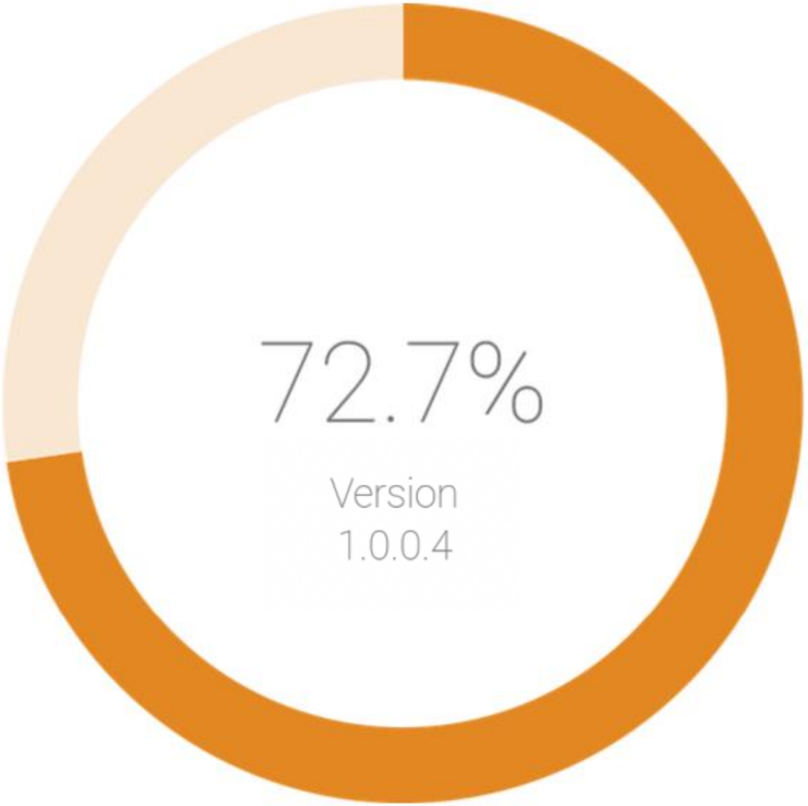
SECURITY IS A MOVING TARGET

Maintaining Visibility and Secure Configuration

Q1 2020 Security Posture



Q3 2020 Security Posture

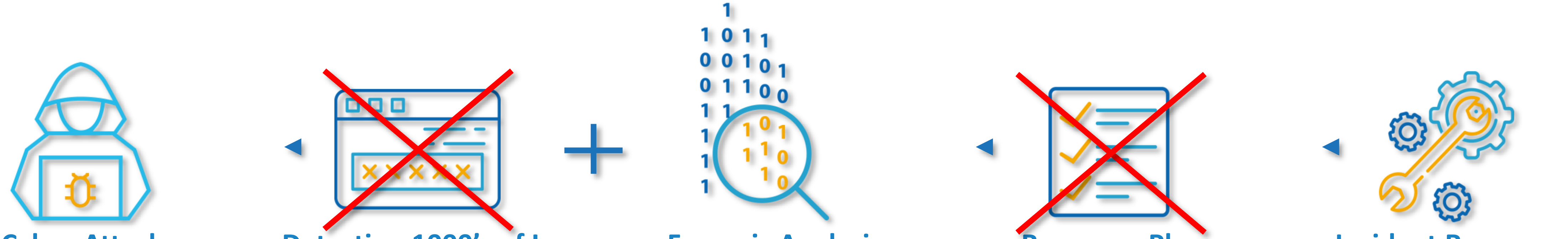


Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

TOO MUCH INFORMATION, TOO LITTLE TIME

Faster Response Needed



Cyber-Attack	Detection 1000's of Logs	Forensic Analysis	Response Plan	Incident Response
TYPICALLY	MONTHS	DAYS	WEEKS	MONTHS
GOAL!!!	IMMEDIATE	IMMEDIATE	IMMEDIATE	IMMEDIATE

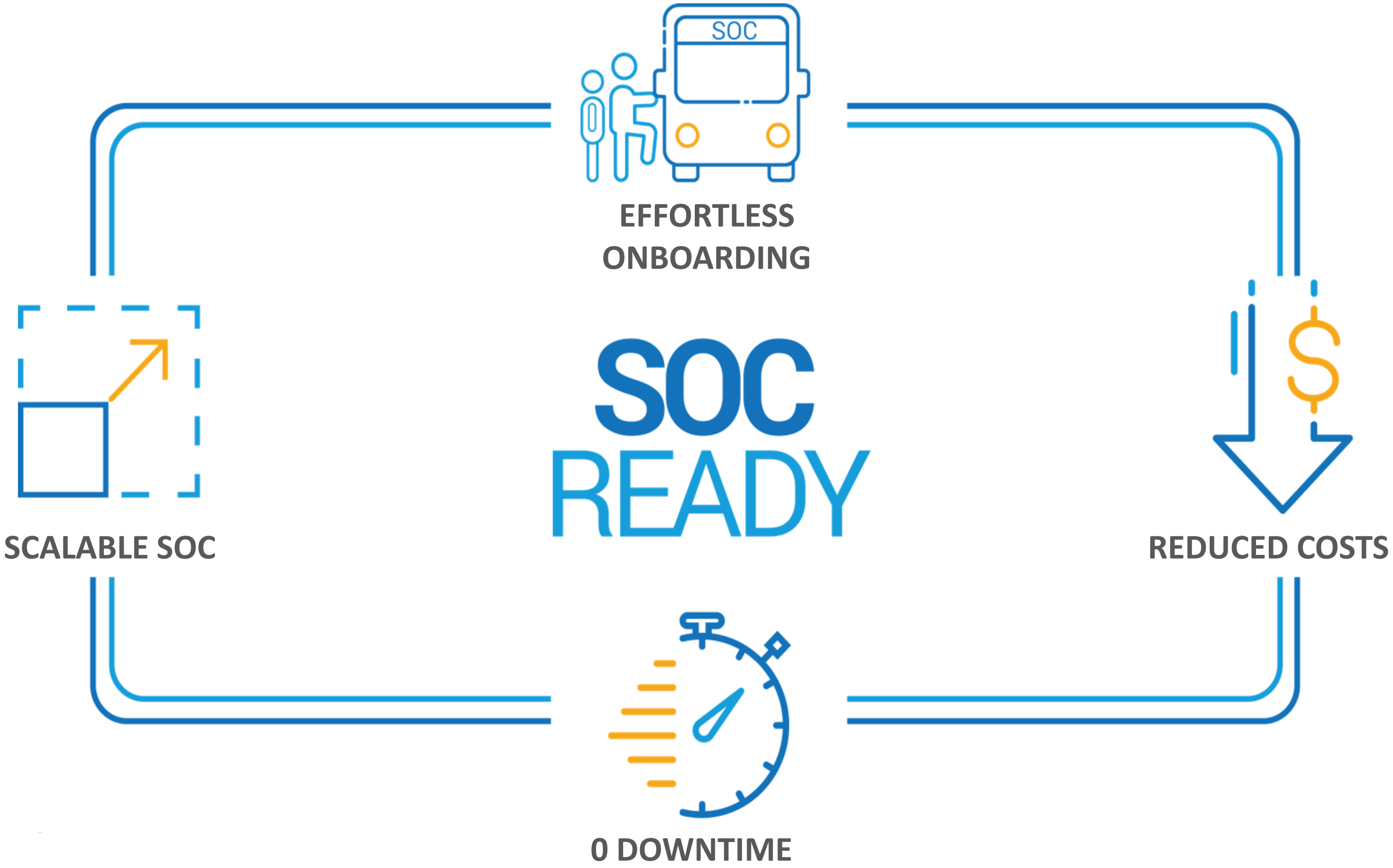
Crown Commercial Service *Supplier*

Medicare Network

More intelligent, More Secure

MONITORING DEVICES EFECTIVELY

Connecting Devices to Security Operation Centre



Crown Commercial Service
Supplier

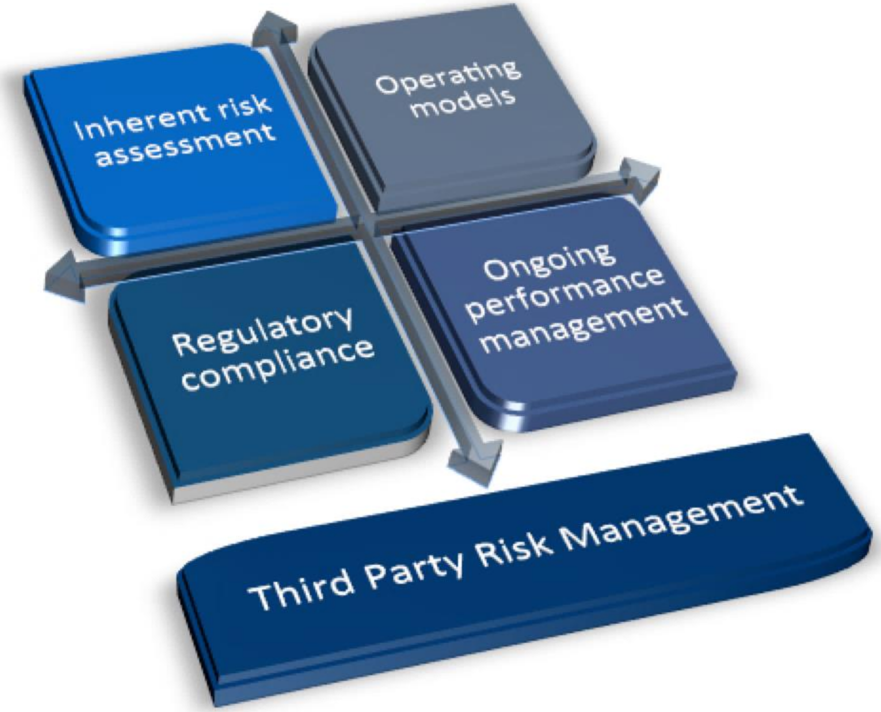
THIRD-PARTY RISK MANAGEMENT

> Third-party suppliers play a critical role in healthcare undergoing digital transformation. Embracing new technologies, supply chains are becoming increasingly integrated and raise an organisation’s operational risk profile on an ongoing basis, if not managed.

THIRD-PARTY SUPPLIERS

Playing a Critical Role in Healthcare

Third-party suppliers are essential partners to healthcare providers and have become **increasingly reliant on them to deliver critical processes and services**, that cannot realistically be produced or replicated in-house.



Crown Commercial Service
Supplier

Medicare Network
More intelligent, More Secure

SUPPLIER ASSESSMENTS

Supply Chain Risk Management

- Many healthcare providers still use archaic, manual risk management processes that are time-consuming, expensive, and inefficient to assess partnership risks.
- As a result, many prospective third-party suppliers are quickly funnelled through the approval system without receiving adequate examination, introducing a host of cyber security risks.

Provide standardised on-boarding, due diligence, inherent risk calculation, oversight and off boarding of third-party products, services and outsourcing arrangements.

Due diligence and monitoring enables healthcare providers to maintain risk information and questionnaire responses used to generate risk scores and drive remediation.

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

CYBER RESILIENT SUPPLIER RELATIONSHIPS

Manage Relationships to Reduce Risk Exposure

- As the healthcare industry continues to advance, new strategies, tools and safeguards must be developed to protect clinical environments, reduce risks, and mitigate threats to highly sought-after healthcare data.
- The ultimate goal is patient safety, therefore an effective cyber security solution is essential to continuously assess security threats facing healthcare to prevent unauthorised access, the reality is that data breaches are inevitable.
- Contract reviews for new regulatory requirements, including SLA reviews are essential.

Crown Commercial Service *Supplier*

Medicare Network
More intelligent, More Secure

FINAL MESSAGE

> Viewing cyber security as a **business differentiator,** and as a further means of protecting **patient's safety** requires **different thinking** and **needs to be at the heart** of healthcare digital transformation.

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

THANK YOU FOR JOINING US!

Supporting Digitalisation and Digital Transformation in Healthcare

Medicare Network Contacts

Christopher Dean
christopher.dean@mednetsec.com

Simon Black
simon.black@mednetsec.com

Office Contact Numbers

UK	+44 (203) 355-3785
US	+1 (702) 605-4601

Enquiries
clientservices@mednetsec.com

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure

GLOSSARY

Abbreviations

ACRONYMS	
APT	Advanced Persistent Threat
AI	Artificial Intelligence
CVE	Common Vulnerability Enumerator
DSPT	Data Security and Protection Toolkit
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation (Directive)
HIDS	Host-Based Intrusion Detection System
IOMT	Internet of Medical Things
IOT	Internet of Things
IPS	Intrusion Prevention Systems
MDM	Medical Device Manufacturer
MDR	Medical Devices Regulations

ACRONYMS	
MHRA	Medicines and Healthcare products Regulatory Agency
NCSC	National Cyber Security Centre
NIS	Network and Information Systems (Directive)
NIST	National Institute of Standards and Technology
OT	Operational Technology
RPM	Remote Patient Monitoring
SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operation Centre
VEX	Vulnerability and Exploitability
VPT	Vulnerability Prioritisation Technology

Crown
Commercial
Service
Supplier

Medicare
Network
More intelligent, More Secure