The State of the Threat Landscape in the Healthcare Industry

Duncan Brown
EMEA Chief Security Strategist

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Health

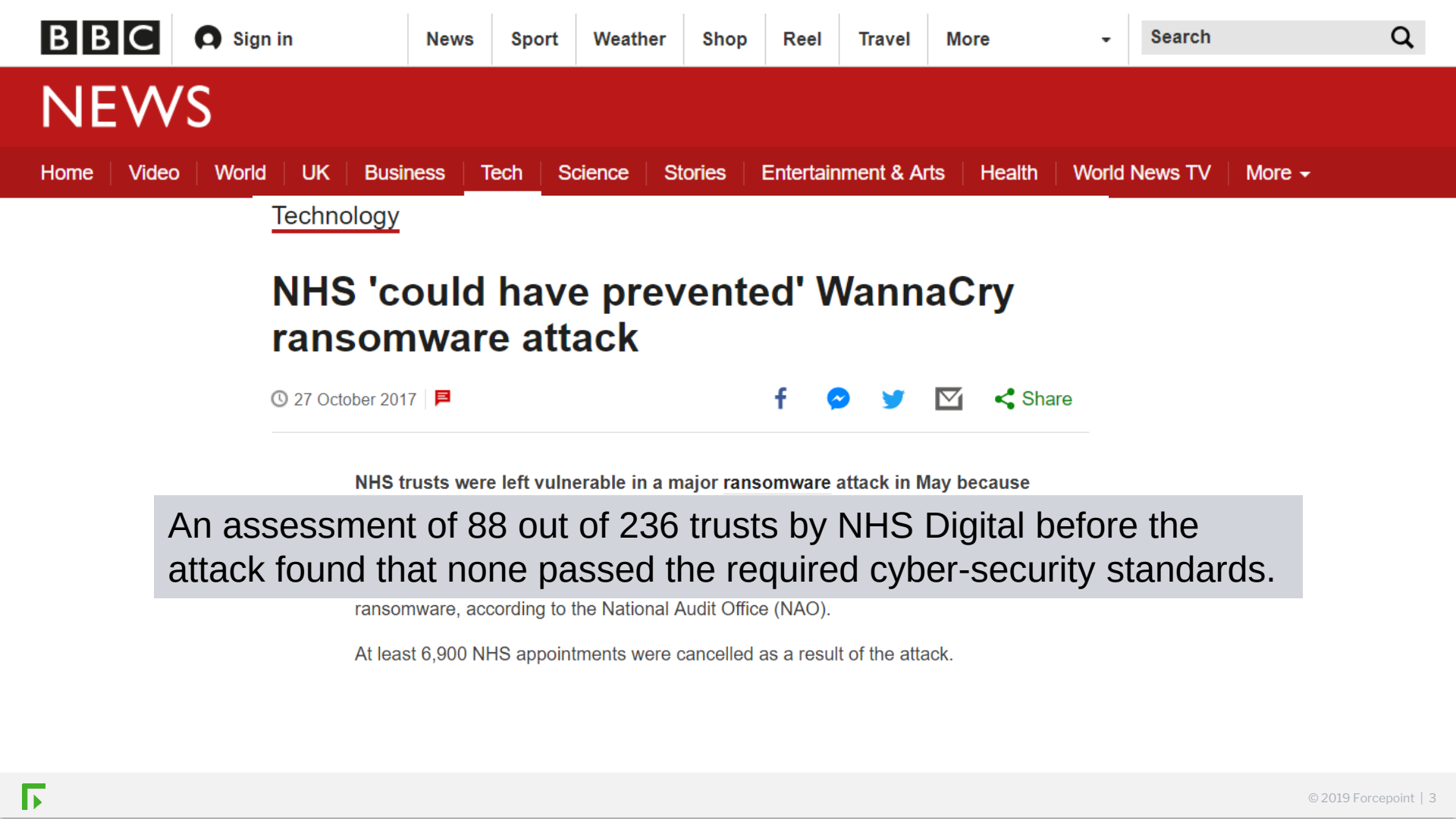
NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017 Share

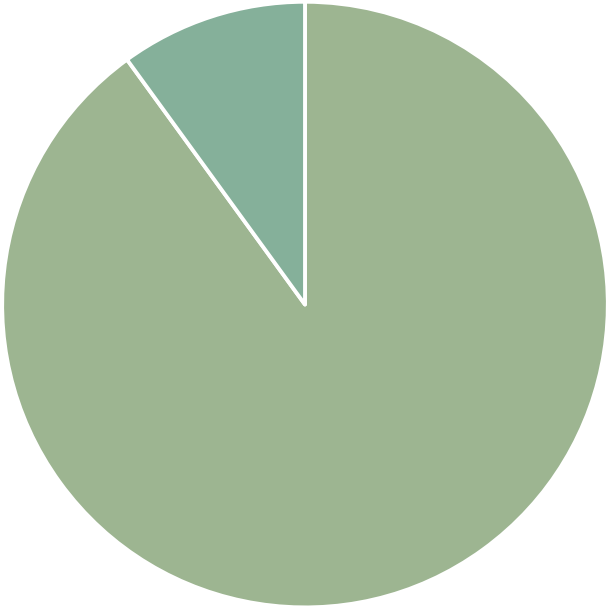
NHS services across England and Scotland have been hit by a large-scale cyber-attack that has disrupted hospital and GP appointments.

The prime minister said the incident was part of an untargeted wider attack **affecting organisations globally.**

Some hospitals and GPs have been unable to access patient data, after their computers were locked by a ransomware program demanding a payment worth £230.


BBC
Sign in
News
Sport
Weather
Shop
Reel
Travel
More
Search
NEWS
Home
Video
World
UK
Business
Tech
Science
Stories
Entertainment & Arts
Health
World News TV
More
Technology
NHS 'could have prevented' WannaCry ransomware attack
27 October 2017
Share
NHS trusts were left vulnerable in a major ransomware attack in May because
An assessment of 88 out of 236 trusts by NHS Digital before the attack found that none passed the required cyber-security standards.
ransomware, according to the National Audit Office (NAO).
At least 6,900 NHS appointments were cancelled as a result of the attack.

There’s a problem with inertia…



Freedom of Information request revealed that 90% of (UK) hospitals still had machines running on Windows XP.
Source: Citrix, reported by BBC

The four ‘C’s of Inaction:

- Compatibility
- Complexity
- Criticality
- Complacency

TECH

Facebook sent a doctor on a secret mission to ask hospitals to share patient data

- Facebook was in talks with top hospitals and other medical groups as recently as last month about a proposal to share data about the social networks of their most vulnerable patients.
- The idea was to build profiles of people that included their medical conditions, information that health systems have, as well as social and economic factors gleaned from Facebook.
- Facebook said the project is on hiatus so it can focus on "other important work, including doing a better job of protecting people's data."

Christina Farr | @chrissyfarr

Published 2:01 PM ET Thu, 5 April 2018 | Updated 11:46 AM ET Fri, 6 April 2018

CNBC

Huge Singapore data breach shows need for new approach

A major data breach in Singapore underlines the need for a new approach to protecting critical data and applications, say security experts

Warwick Ashford
Security Editor

20 Jul 2018 16:45

Personal data of 1.5 million citizens, including prime minister Lee Hsien Loong, has been stolen from a government health database in Singapore in a “deliberate, targeted and well-planned attack”, according to health ministry.

Those affected visited SingHealth’s specialist outpatient clinics and polyclinics from 1 May 2015 to 4 July 2018, but while data includes names, addresses, gender and date of birth, no medical records were involved apart from details of medicines dispensed to about 160,000 patients, the health ministry said in a statement.

They subsequently managed to obtain privileged account credentials to gain privileged access to the database, the agency said, adding that upon discovery, the breach was immediately

Nurse prosecuted for inappropriately accessing patient records

Date **25 September 2018**
Type **News**

A former nurse at Southport and Ormskirk Hospital NHS Trust has been prosecuted for accessing patients' medical records without authorisation.

[redacted] who had been a staff nurse on the hospital's Rehabilitation Ward since October 2011 had accessed patients' medical records outside of her role.

The Court heard that [redacted] had inappropriately accessed the records – including maternity and paediatric records - of five patients, 17 times.

She also accessed a further 109 records of 18 patients of which one was a child. The activity occurred between 2014 and 2016.

First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay €400,000 GDPR Fine

Home | GDPR News | First Hospital GDPR Violation Penalty Issued: Portuguese Hospital to Pay

- 985 active doctor accounts, but only 296 doctors
- All doctors had access to all patient records
- Hospital argues that the Health Ministry is responsible

Posted By HIPAA

for failing to restrict access to patient data stored in its patient management system.

Concerns were raised about the lack of data access controls in April 2018. Medical workers in the southern zone discovered non-clinical staff were using medical profiles to access the patient management system.

CNPD conducted an audit of the hospital and discovered 985 hospital employees had access rights to sensitive patient health information when there were only 296 physicians employed by the hospital. Only medical doctors at the hospital should have been able to access that level of detailed information about patients. CNPD also discovered a test profile had been set up with full, unrestricted administrator-level

Personal records of HIV-positive individuals in Singapore leaked online

The personal information of 14,200 people with the human immunodeficiency virus was leaked by an American who lived in Singapore

Aaron Tan
TechTarget
29 Jan 2019 4:53

The personal information of 14,200 people in Singapore with HIV (human immunodeficiency virus) was reportedly leaked online in yet another data breach that has come to light in the city-state.

According to Singapore's Ministry of Health (MOH), the information included the names, identification numbers, contact details, HIV test results and related medical information of 5,400 Singaporeans and 8,800 foreigners diagnosed with HIV in Singapore.

The information was leaked by Mikhy K Farrera Brochez, a HIV-positive male American who was residing in Singapore, on an employment pass, between January 2008 and June 2016.

He allegedly gained access to the information through his Singaporean partner Ler Teck Siang, the head of MOH's National Public Health Unit who was authorised to access information in the

19TH FEBRUARY 2019 11:28AM

CYBERSECURITY

Swedish Healthcare breaches GDPR in leak of 2.7 million patient call recordings

Swedish Healthcare Guide, a telephone service that provides Swedes with healthcare information, is likely to be in breach of GDPR after it was discovered that 2.7 million unique voice recordings from the service had been left on an unencrypted, publically accessible server.

The server, which was used to store recordings of phone calls to the Swedish Healthcare Guide service in real-time, held over 170,000 hours of calls. Some dated back as far as 2013.

Many of the calls include the discussion of sensitive healthcare details, while some include social security numbers. A small percentage of the files even include phone numbers in the file names.

Lucy Ingham

Lucy is the editor of Verdict.
You can reach her at
lucy.ingham@pmgoperations.com

POPULAR TODAY

1

TechCrunch

Dozens of companies leaked sensitive data thanks to misconfigured Box accounts

Zack Whittaker @zackwhittaker / 1 week ago

Comment

- United Tissue Network, a whole-body donation nonprofit, exposed body donor information and personal information of donors in a vast spreadsheet, including the prices of body parts.

data stored in Box enterprise accounts is private by default, users can share files and folders with anyone, making data publicly accessible with a single link. But Adversis said these secret links can be discovered by others. Using a script to scan for and enumerate Box accounts with lists of company names and wildcard searches, Adversis found more than 90 companies with publicly accessible folders.

Not even Box's own staff were immune from leaking data.

HEALTHCARE, UAE

Dubai Healthcare City unveils first telehealth platform

ADELLE GERONIMO
FEBRUARY 3, 2019, 10:20 AM

The Dubai Healthcare City, DHCC, has announced the first regulated telehealth platform in the free zone.

The new service was launched through a live consultation between a patient at Arab Health, a healthcare conference and trade show, and a licensed doctor in the free zone.

The initiative is in line with the Fifty-Year Charter of Sheikh Mohammed bin Rashid Al Maktoum, Vice President, Prime Minister and Ruler of Dubai, and seeks to provide a doctor for each citizen. It aims to make available doctors, specialists and medical

GULF NEWS

GOVERNMENT

Dh700,000 fine for sharing patient's information without permission

FNC passes new law to ensure privacy of patient's data by all medical and health care professionals, and facilities

Published: October 30, 2018 18:47

Samir Salama, Associate Editor

Abu Dhabi: Publishing a medical advertisement without a licence will attract a fine of between Dh100,000 and Dh200,000, according to a new Federal Bill passed yesterday (Tuesday) by the Federal National Council.

The new legislation also prohibits handling, transferring or storing of medical records and health information outside the country. Those who violate this article will face a fine ranging between Dh500,000 and Dh700,000.

Lessons

- Do the basics well:
  - Access control, encrypted passwords, patching, basic security hygiene.
- Know what data would hurt you – or your patients/customers – if you lost it:
  - Some data is more important than other data…
- Encrypt the data!
  - Lost encrypted data is ***not*** lost data!
- Complacency is your enemy!
  - Check and test and verify, then check again.
- ***You*** are responsible for the data under your control
  - Beware of “Shared Responsibility” clauses…

Human-Centric Security For The Era Of Digital Transformation

Duncan Brown
EMEA Chief Security Strategist

FORCEPOINT

Data Protection | Web Security | CASB | NGFW | Advanced Malware Detection | Behavioral Analytics | Insider Threat | Email Security | Data Guard | Cross Domain

Data and medicine

A revolution in health care is coming

Welcome to Doctor You

Print edition | Leaders ›
Feb 1st 2018

Digital Transformation Will Unlock Tremendous Value… If Cybersecurity Challenges Can Be Addressed

$100 trillion

The value that the World Economic Forum estimates will be created from digitalization over the next 10 years.

Source: Digital Transformation Initiative, World Economic Forum, May 2018.

"What are the greatest challenges in digital transformation?"

Security	**31%**
Technology strategy	24%
Company culture	23%
Lack of technology skills	20%

Source: Forrester: The Sorry State Of Digital Transformation in 2018.

Four Elements Of Digital Transformation That Create Advantage And Risk

box workday. salesforce Office 365

"Your IT infrastructure is going to the cloud, driven by business need and speed."

- Cloud IT creates security blind spots and fragmented security management and accountability.

"Data is the new oil and artificial intelligence the new engine of the digital economy."

- More critical data is being created than properly protected.
- Data should flow freely across the business.

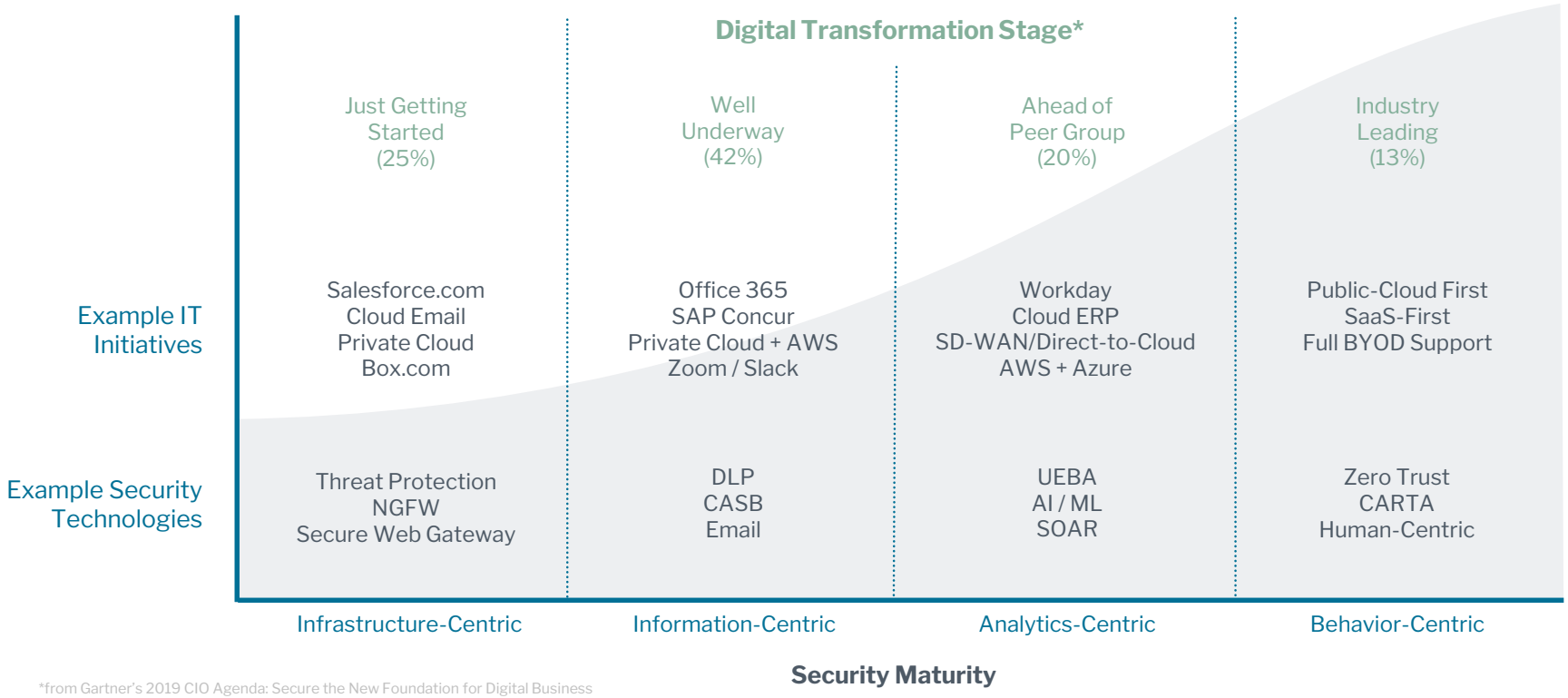
"Workforce, devices, and business processes are globally hyperconnected."

- Network transformation to support cloud-centric IT breaks existing security architectures.
- Personal and IoT devices are security vulnerabilities.

"Employees and partners collaborate using all of a company's assets."

- A critical need is created to ensure trusted interactions across the extended enterprise.

Where Are You In Your Digital Transformation Journey?



*from Gartner's 2019 CIO Agenda: Secure the New Foundation for Digital Business

Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA)

"We need security infrastructure and security decisions to become continuous and adaptive – enabling real-time decisions that balance risk, trust and opportunity and the speed of digital business."

"We must have visibility into what the entity – the user – is doing once it gains access. How is it behaving? Does the entity or its behaviors represent excessive risk? If so, then we should have the ability to detect this, confirm that it is real, prioritize it and take action."

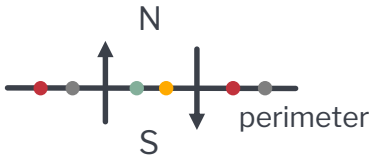
Neil MacDonald, Gartner Research Note G00351017, April 10th 2018

What is the best way to reduce risk and secure an environment you increasingly don't own or fully manage?

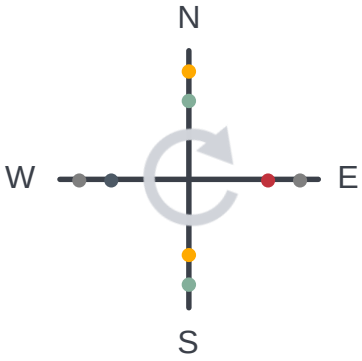
Humans and Data

Users And Data Must Be At The Center Of Your Design Thinking

User and data interactions are distributed, diverse and dynamic – this breaks traditional security architectures and increases business risk



Network-Centric



Virtual & App-Centric

User & Data Centric

Pre-2000 → Infrastructure-centric → **2010** → Behavioral-centric → **2020**

Users And Data Must Be At The Center Of Your Design Thinking

User and data interactions are distributed, diverse and dynamic – this breaks traditional security architectures and increases business risk

Traditional Security

One-to-many enforcement of static, generic policies, producing high false positive rates.

User & Data Centric

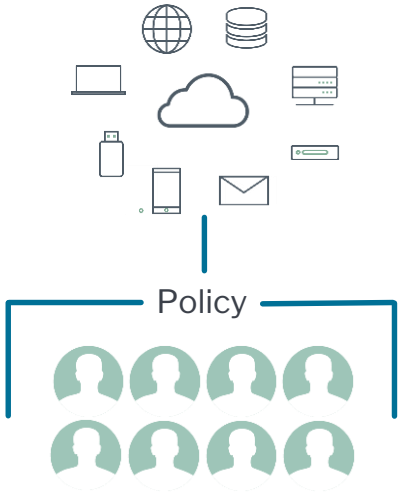
Degree of Digital Transformation

IT Complexity & Risk

Pre-2000 → Infrastructure-centric → 2010 → Behavioral-centric → 2020

Human-Centric Cybersecurity Changes Everything

Traditional Security



One-to-many enforcement of static, generic policies, producing high false positive rates.

Human-Centric Security

One-to-one enforcement of different policies based on the risk, enabling automation.

Risk-Adaptive In Action

Senior Health Practitioner, Dubai

Monday
January 21 @ 10am

Working while on PTO

+ Additional Context

Risk Score: 30

Risk-Adaptive Protection

No enforcement action

Thursday
January 24 @ 1pm

Downloads patient records to Excel

+ Additional Context

Risk Score: 50

Risk-Adaptive Protection

Enhanced auditing activated

Evidence available for investigation later

Wednesday
January 30 @ 9pm

Copy multiple files to staging area

+ Additional Context

Risk Score: 80

Risk-Adaptive Protection

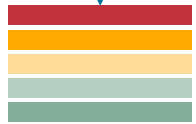
Copy allowed but file encrypted

No corporate data at risk

Saturday
February 9 @ 6am

Bulk copy to USB drive

+ Additional Context



Risk Score: 95

Risk-Adaptive Protection

Action is blocked & account is locked

Avoided $10M breach and forensic proof of the attack is available

Thank you

duncan.brown@forcepoint.com