unitec
Accessible Expertise

Colin Butler

Unitec IT Solutions

CYBER SECURITY EVENT


Managed Services


IT Infrastructure


Cloud Computing


Telecoms


Security


Disaster Recovery

unitec
Accessible Expertise

- Type of attack (phishing, ransomware, DDoS, insider threat)
- Entry point (weak passwords, unpatched systems, employee click)

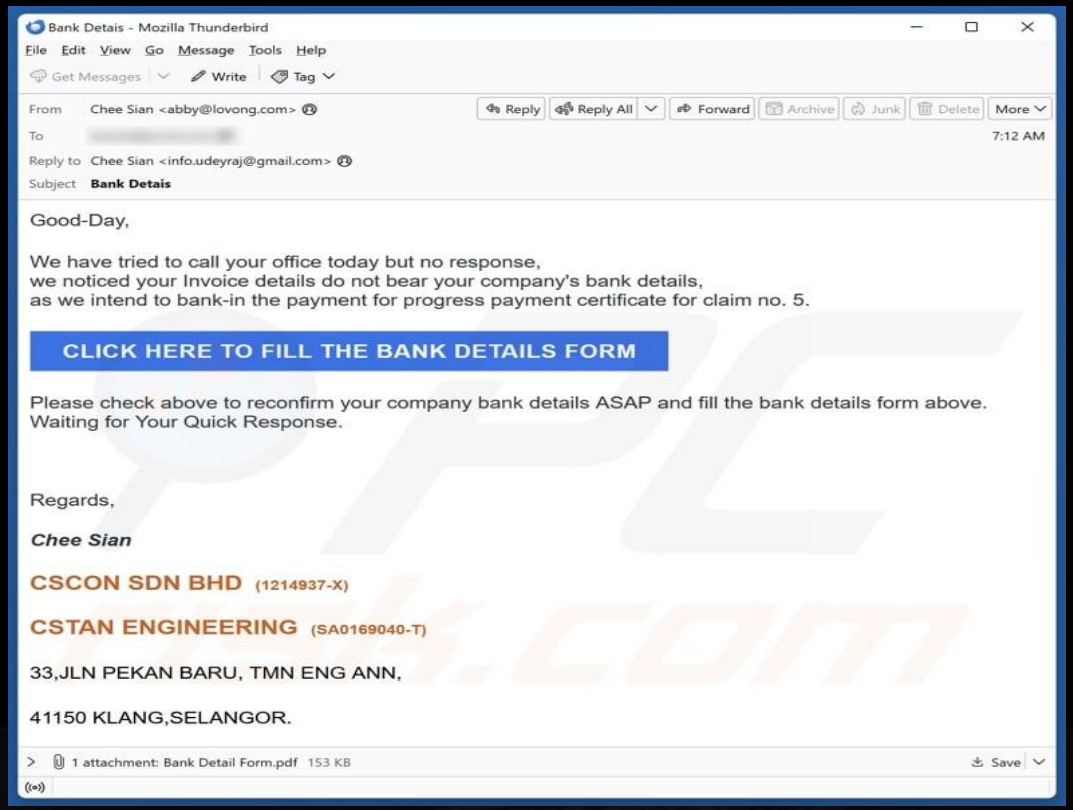
Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

MAILBOX BREECH

The most common we see

Example

- Company A gets a mail from Company B to say they are changing bank accounts details
- CA just updates the payment details
- Bad Actor sent the mail from CB after intercepting the invoice sent from CA
- Because CA didn't verify, a payment was made to the bad actor’s bank account instead of CB
- CB only finds out that €450k is missing when CA chases a late payment



Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

WEBSITE PHISHING

unitec
Accessible Expertise

Example

- User visits a website but misspells the site by one character
- The bad actor has set-up a similar website, and captures the user's username and details
- The bad actor even captures the MFA request when the real site requests it
- Now the bad actor has all the credentials to access not only the details on the site, but also any associated accounts

Managed Services
IT Infrastructure
Cloud Computing
Telecoms
Security
Disaster Recovery

RANSOMWARE

The most devastating attack a company can face

unitec
Accessible Expertise

Example

- Bad actor uploaded a payload into MS365 on a remote site
- Over several months, the bad actor worked their way to the main HQ site where the servers resided
- They elevated rights to give themselves admin privileges
- Then they stole the company personal/accounts data - full of payroll and employee details

Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

RANSOMWARE

The most devastating attack a company can face

Continued

- The company data was held to ransom for $800k
- Thankfully, the company DR systems and processes brought them back in 3 days
- The ransomware wasn't paid
- What happened next caused disruption for weeks

unitec
Accessible Expertise

Managed Services

IT Infrastructure

Cloud Computing

Telecoms

Security

Disaster Recovery

RANSOMWARE

The most devastating attack a company can face

Continued

- The bad actors cloned the MD's Mobile Phone number
- Called employees confirming personal details and threatening to release online
- The FC was threatened if the ransom wasn't paid
- Again, the ransom wasn't paid
- Staff goodwill got the business through the incident

unitec
Accessible Expertise

Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

unitec
Accessible Expertise

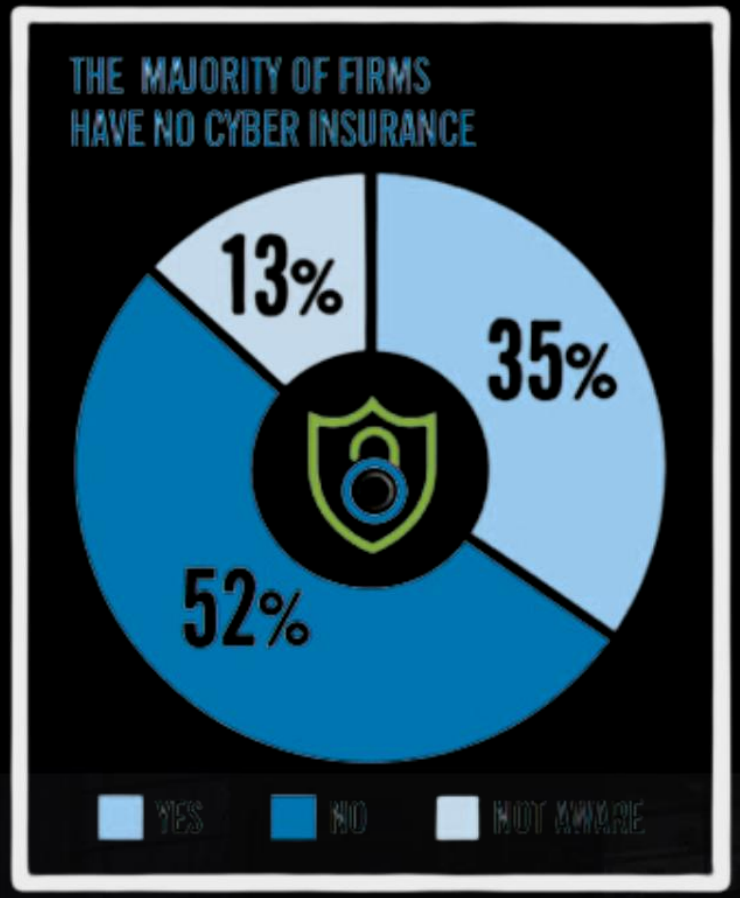
WHY THE ATTACK HAPPENED

- Motivation of attackers (financial gain, espionage, activism)
- Targeted vs. opportunistic.
- Industry risks (e.g., healthcare = sensitive data, retail = card info)
- Reason for our case study?

Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

unitec
Accessible Expertise

1 29% REPUTATIONAL LOSS
2 26% MANAGEMENT TIME
3 16.4% CUSTOMER LOSS OR CHURN
4 12% CLEAN-UP COSTS
5 7.4% DIRECT LOSS OF TURNOVER
6 3.6% COMPETITIVENESS
7 3.1% CUSTOMER BEHAVIOUR CHANGE



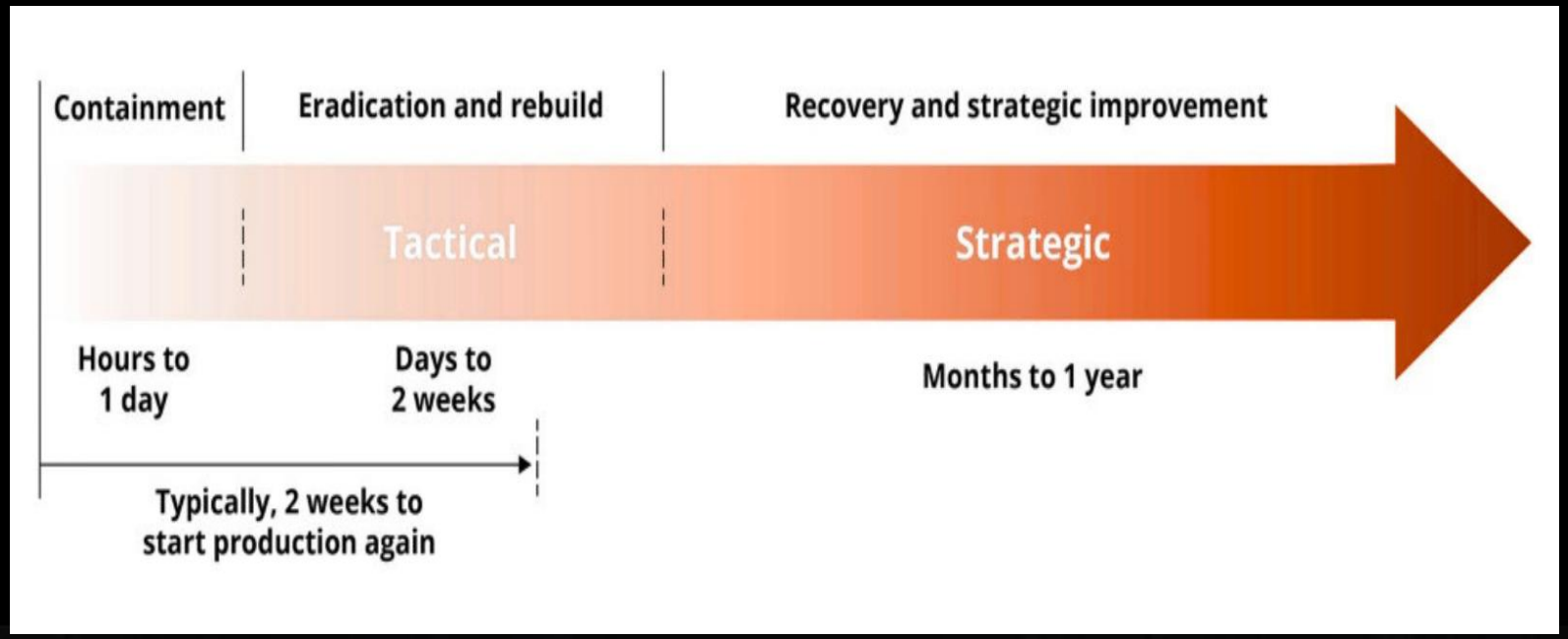
IMMEDIATE IMPACT

- Downtime (hours/days)
- Systems affected
- Operations halted (e.g., website down, production stopped)

Managed Services
IT Infrastructure
Cloud Computing
Telecoms
Security
Disaster Recovery

DOWNTIME STATISTICS

- Average downtime for similar incidents (industry benchmarks)
- Specific downtime suffered by victim
- Steps taken (incident response, patching, backups)
- Time to full recovery
- Costs of recovery (IT staff, consultants, new security tools)



Managed Services | IT Infrastructure | Cloud Computing | Telecoms | Security | Disaster Recovery

COSTS BY SECTOR

BUSINESS SIZE	COST PER INCIDENT AVG.*
SMEs (9–50 employees)	**€25,000** per incident
Large incidents (corporate)	**€135,000** per incident
Cleanup/remediation	**€29,954** average
HSE (State health sector)	**€52 million–€100 million** total

*Cost increasing rapidly each year

LOST EARNINGS & FINANCIAL IMPACT

- Estimated lost revenue during downtime
- Extra costs (legal, PR, ransom payments)
- Long-term impact (customer churn, fines, brand damage)
- Loss calculated for case study?


Managed Services


IT Infrastructure


Cloud Computing


Telecoms


Security


Disaster Recovery

LESSONS LEARNED FROM CYBER ATTACKS

NO ONE IS TOO SMALL TO BE A TARGET

Many SMEs assume hackers only go after big corporations, but studies show over 40% of cyberattacks targer small businesses

PREVENTION IS CHEAPER THAN RECOVERY

The HSE ransomware attack in Ireland cost tens of millions in recovery, but experts say proactive investment in security tools and staff training would ve been far less costiy

HUMAN ERROR IS THE WEAKEST LINK

Phishing and social engineering remain the #1 entry point for attacks

BACKUPS AND DISASTER RECOVERY ARE CRITICAL

Organizations that had offline; fested backups recovered faster after ransomwre atracks

INCIDENT RESPONSE PLANS SAVE TIME AND MONEY

REGULATORY AND LEGAL RISKS ARE REAL

Under GDPR. Irish firms face fines, for failing to protect customer data

TRANSPARENCY BUILDS TRUST

The HSE learned that poor communication quring its rancomware affack worsened public trustration

THIRD-PARTY RISKS CAN'T BE IGNORED

Many breaches stem from compromised vendors, contracters, or partners

CYBER INSURANCE IS HELPFUL BUT NOT A SILVER BULLET

Insurance may cover ransom payments or recovery costs, but it canner replace *lost* trust or reputational damage

CYBERSECURITY IS ONGOING, NOT ONE-OFF

Yesterday's defenses may not stop tomorrow's attack.