unitec
Accessible Expertise

‹Plug Us In

Welcome

Unitec IT Solutions

CYBER SECURITY EVENT

CYBER RISK IN IRELAND 2026

Why Irish businesses are under increasing cyber threat

unitec
Accessible Expertise
Plug Us In

THE SCALE OF THE PROBLEM

1 in 3
Irish SMEs attacked



5,200+
Cyber incidents recorded

721
Confirmed malicious attacks

THE FINANCIAL IMPACT

€22,773 Average SME ransom

€50,000 Average annual SME cyber cost

€683,000 Average enterprise ransom payment

THE NEW THREAT LANDSCAPE



81%
of phishing emails are AI-assisted



22.6%
rise in phishing-delivered ransomware

7.2 MILLION
workdays lost every year

due to cyber incidents and downtime

29%
of large firms paid a ransom

Cybercrime is no longer an IT issue. It is a business risk.

Sources: Garda National Cyber Crime Bureau • RTÉ • Expleo Ireland • Microsoft • Cybersecurity industry reports

unitec
Accessible Expertise

‹Plug Us In

Stephen Wright

Senior Director, Security Compliance & Assurance

Governance, Risk & Compliance (GRC)

Dell Technologies | Security & Resiliency Organization (SRO)

CYBER SECURITY EVENT

unitec
Accessible Expertise

‹Plug Us In

Colin Butler

Head of Sales & Marketing, Unitec

CYBER SECURITY EVENT

unitec
Accessible Expertise

‹Plug Us In

WELCOME

Clients, businesses, co-organisers, supply partners and friends

Unitec Team

Special Thanks:

- Dell (Gemma Lane & Team)
- Regional Skills Mid-West (Joe)
- Supply partners



unitec
Accessible Expertise
Plug Us In

AGENDA OF TOPICS

- 10.00am: Welcome (Dell)
- 10.05am: Unitec
- 10.25am: Regional Skills
- 10.35am: Garda NCCB
- 10.45am: Unitec NIS 2.0
- 10.55am: Fortinet
- 11.05am: Huntress
- 11.15am: Datto/Kaseya
- 11.25am: Mesh
- 11.35am: uSecure
- 11.45am: MS Copilot
- 11.55am: Unitec looking ahead
- 12.00pm: Q&A, Lunch
- 1.00pm: Innovation Centre tour

unitec
Accessible Expertise

‹Plug Us In

CHOOSE UNITEC

- Award-winning Irish MSP: Best SME, workplace and inclusion awards
- ISO 27001 and ISO 9001 certified
- Locally owned, with offices in Tipperary, Cork and Waterford
- Personal service, proactive support and quality supplier solutions
- Security testing, ethical hacking and proactive monitoring



CYBER RISK IN IRELAND 2026

Why Irish businesses are under increasing cyber threat

unitec
Accessible Expertise
Plug Us In

THE SCALE OF THE PROBLEM

1 in 3
Irish SMEs attacked



5,200+
Cyber incidents recorded

721
Confirmed malicious attacks

THE FINANCIAL IMPACT

€22,773 Average SME ransom

€50,000 Average annual SME cyber cost

€683,000 Average enterprise ransom payment

THE NEW THREAT LANDSCAPE



81%
of phishing emails are AI-assisted



22.6%
rise in phishing-delivered ransomware

7.2 MILLION
workdays lost every year

due to cyber incidents and downtime

29%
of large firms paid a ransom

Cybercrime is no longer an IT issue. It is a business risk.

Sources: Garda National Cyber Crime Bureau • RTÉ • Expleo Ireland • Microsoft • Cybersecurity industry reports

unitec
Accessible Expertise

‹Plug Us In



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

unitec
Accessible Expertise

Plug Us In

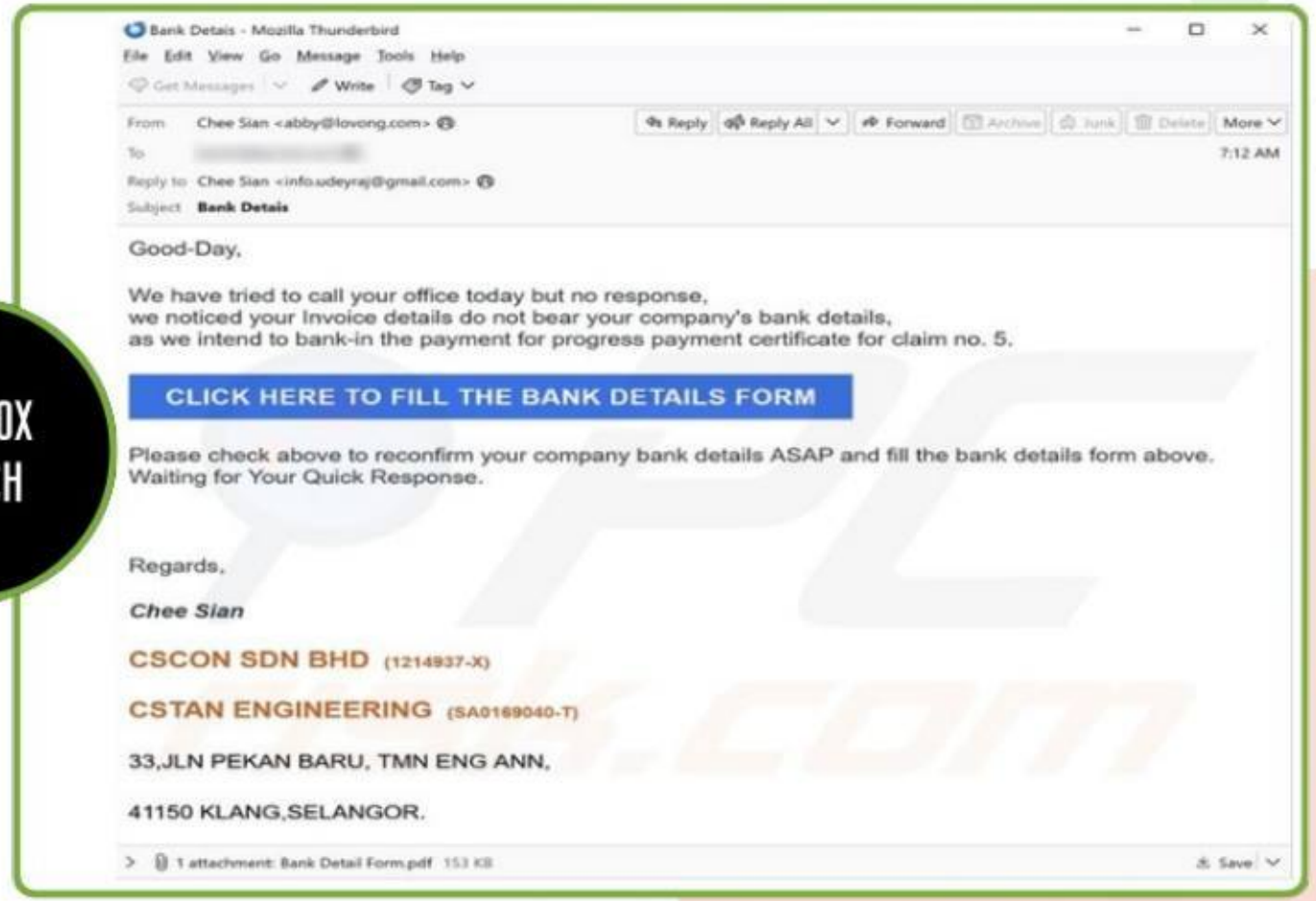
MAILBOX BREECH

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

MAILBOX BREECH



unitec
Accessible Expertise

WEBSITE PHISHING

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



unitec
Accessible Expertise

‹Plug Us In

RANSOMWARE

The most devastating attack a company can face
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



unitec
Accessible Expertise

RANSOMWARE

The most devastating attack a company can fac

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

Plug Us In

RANSOMWARE

The most devastating attack a company can face

Continued

- The bad actors cloned the MDs 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



unitec
Accessible Expertise
‹Plug Us In

WHY THE ATTACK HAPPENED

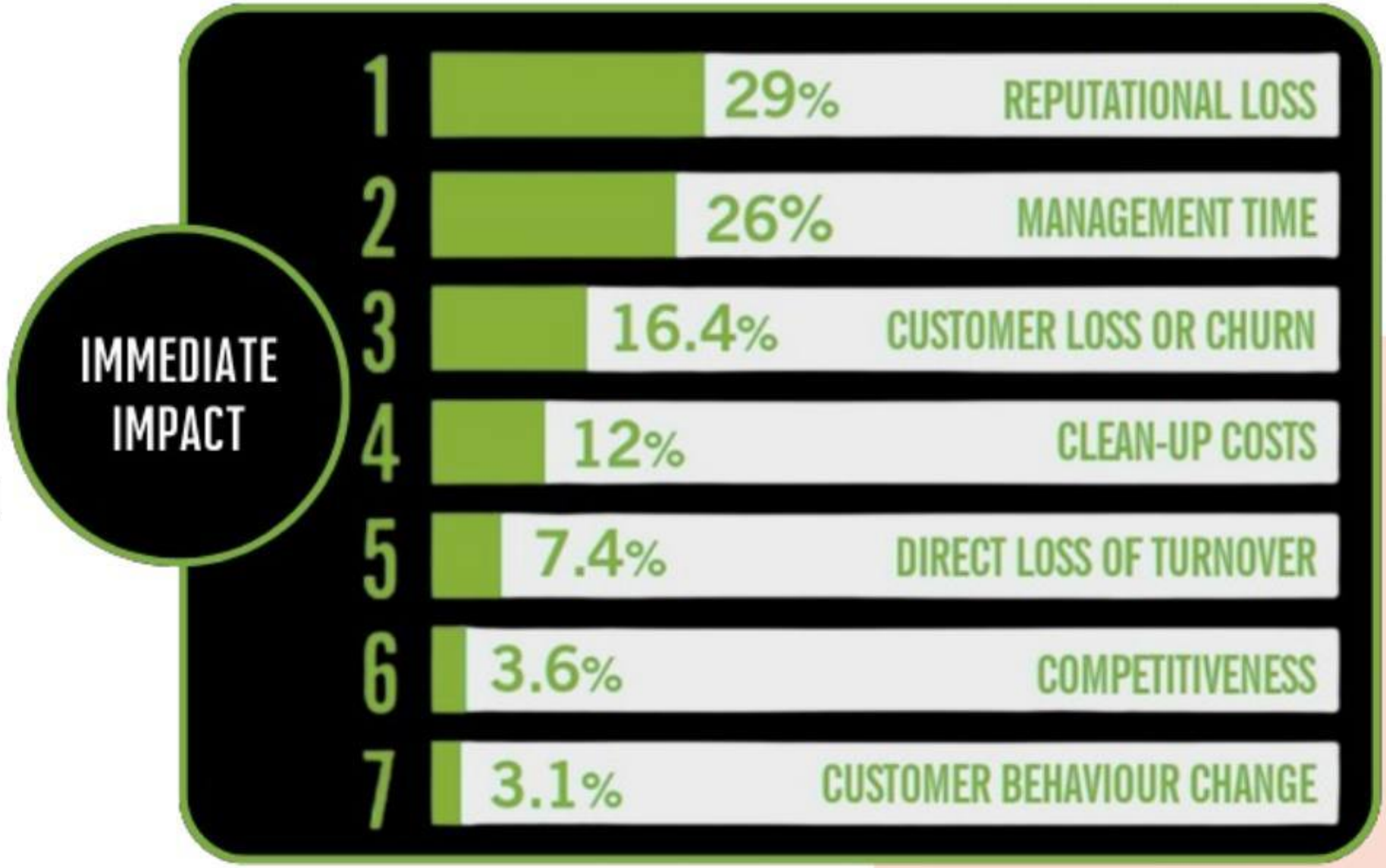
- Motivation of attackers (financial gain, espionage, activism)
- Targeted vs. opportunistic.
- Industry risks (e.g., healthcare = sensitive data, retail = card info)
- Reason for our case



unitec
Accessible Expertise
Plug Us In

IMMEDIATE IMPACT

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



unitec
Accessible Expertise
Plug Us In

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)



unitec
Accessible Expertise

‹Plug Us In

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



LESSONS LEARNED

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.