Insights Report

Human Trust, Now Weaponised AI

A Strategic Briefing for Risk Leaders in Financial Services, Healthcare & Critical Infrastructure

mailguard
A GlobalGuard Company

Executive Summary

Email has become the single most dangerous vector in your business. It delivers the most financially devastating cyberattacks — **Business Email Compromise (BEC), phishing, and ransomware** — while bypassing traditional defences and exploiting one critical vulnerability: **human trust**.

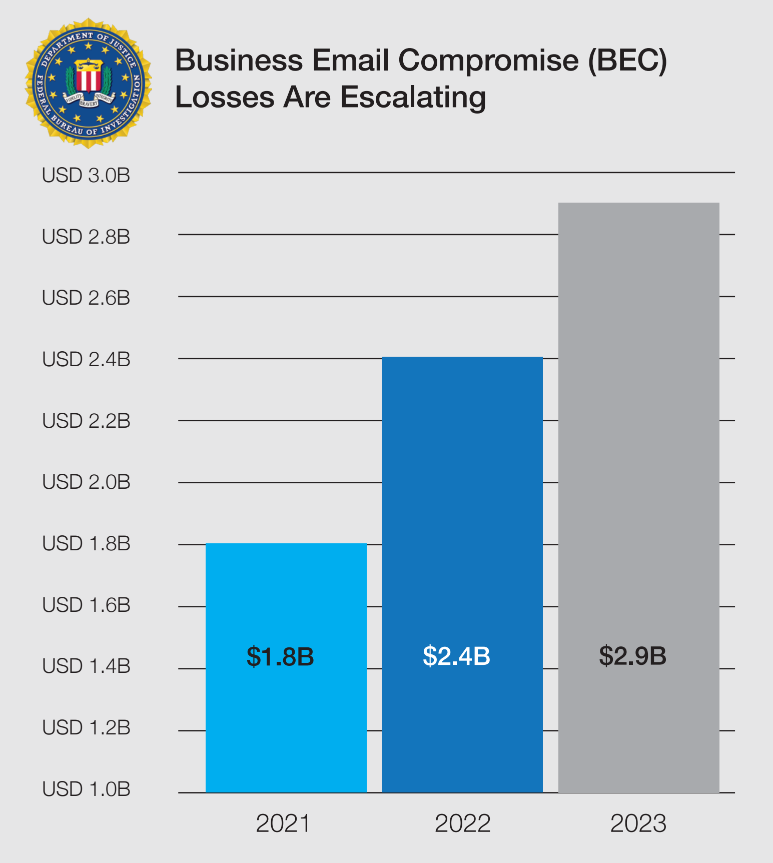
These threats are clean, targeted, and increasingly **generated by AI**. They don't rely on malware — they rely on belief. And when your team clicks, millions of dollars can vanish without anyone knowing.

For CROs, this isn't just a security issue. It's **a fiduciary risk, a regulatory exposure, and an operational liability**.

This report outlines how leading risk executives are addressing this threat — and why speed-to-detect is now a board-level KPI.

Why Email is Now the Number One Risk Vector

- **$2.9B lost to BEC in 2023** — the most damaging cybercrime reported by the FBI.
- **277 days = average breach lifecycle** — attackers lurk undetected for 9 months.
- **95% of breaches involve human error** — mostly from email.
- **AI-generated phishing up 135% in 2023** — removing the signs users are trained to detect.



FBI IC3 Annual Internet Crime Report 2024

References:
https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
https://www.ibm.com/reports/data-breach
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

The Human Factor

Modern email threats no longer solely rely on attachments or malware. They now also weaponise language and context.

The most effective attacks contain no malware, no links, no red flags. That's why they get through — and why your current filters and staff alone can't stop them.

"They didn't hack your system. They hijacked your trust."

— Craig McDonald, CEO & Founder, MailGuard

"BEC exploits human behavior — not technical vulnerabilities."

— Microsoft Security Team, Microsoft DDR 2024

References:
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Human Trust, Now Weaponised by AI

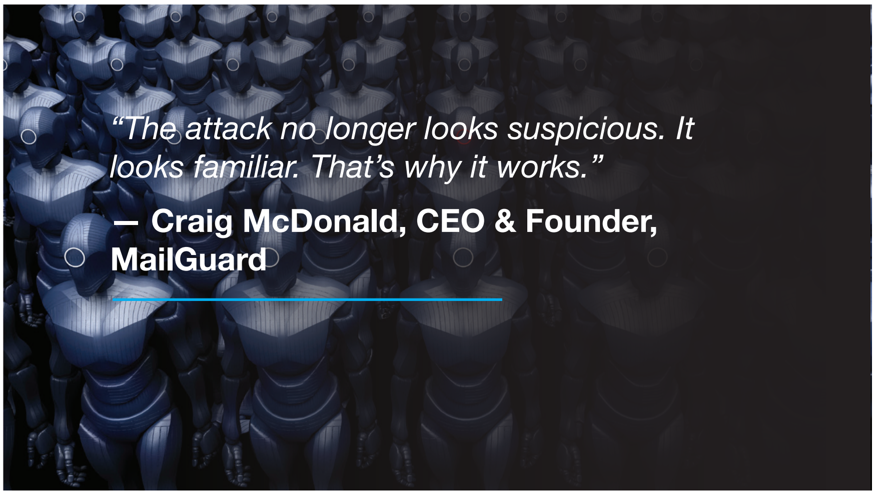
In 2025, attackers now use generative AI to impersonate CEOs, vendors, and even reply to live threads.

- AI crafts emails in a perfect, personalised tone,
- It replicates your CEO’s style,
- Speaks every language,
- Continues threads with stolen context, and
- It never sleeps.

A 2023 CISA study found **AI-generated phishing emails triggered click rates over 60%**, matching human-crafted lures.

And Microsoft reports a **250% spike in BEC attempts** due to AI automation.

Even your best-trained staff can’t stop what they don’t recognise. **If the email reaches the inbox — it’s already too late.**



“The attack no longer looks suspicious. It looks familiar. That’s why it works.”

— Craig McDonald, CEO & Founder, MailGuard

References:
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
https://www.cisa.gov/resources-tools

The Big Three Threats (and Their Costs)

Threat	Description	Financial Impacts
Business Email Compromise (BEC)	Spoofed or compromised accounts requesting transfers	Avg. loss: $129K; many exceed $1M
Phishing	Credential harvesting, fake portals, reply-chain hijacking	Regulatory fines + breach costs
Ransomware	Often starts with phishing; locks data and demands payout	Avg. cost: $5.13M

References:
https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report
https://www.ibm.com/reports/data-breach

Delays Multiply Losses

- Average time to detect + contain breach: **277 days**.
- Breaches detected after 200 days cost **$1M more**.
- Microsoft relies on **Zero-hour Auto-Purge (ZAP)** — which removes threats after delivery.

Time-to-detect (TTD) is no longer a technical metric. It's a financial one.

> *"The only thing more dangerous than a fast attacker is a slow response."*
>
> **— Craig McDonald, CEO & Founder, MailGuard**

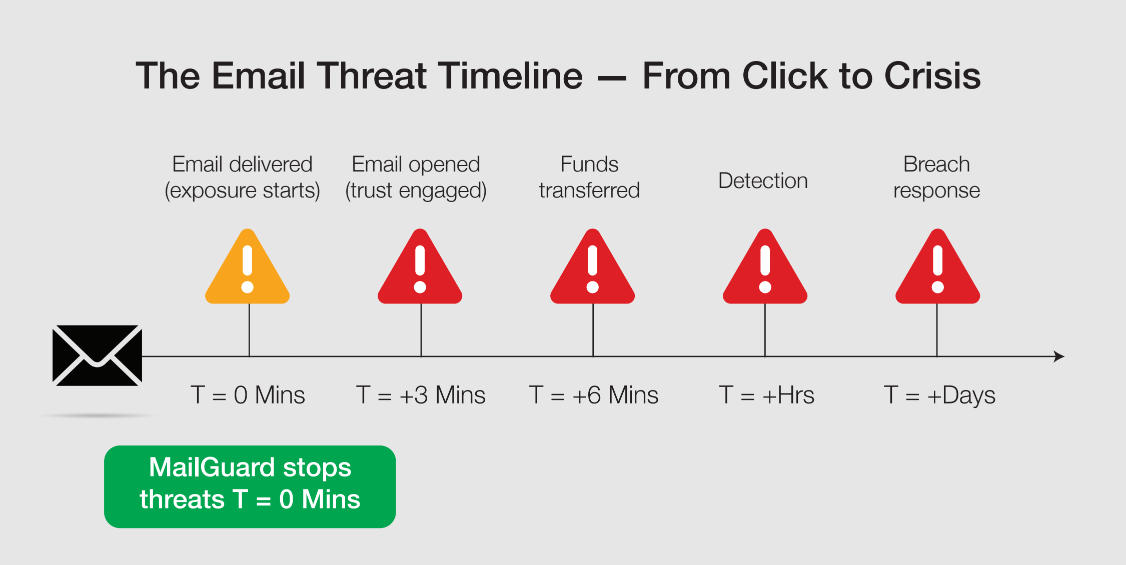

The Email Threat Timeline — From Click to Crisis
Email delivered (exposure starts)
Email opened (trust engaged)
Funds transferred
Detection
Breach response
T = 0 Mins
T = +3 Mins
T = +6 Mins
T = +Hrs
T = +Days
MailGuard stops threats T = 0 Mins

Figure 1 - The Email Threat Timeline - From Click to Crisis

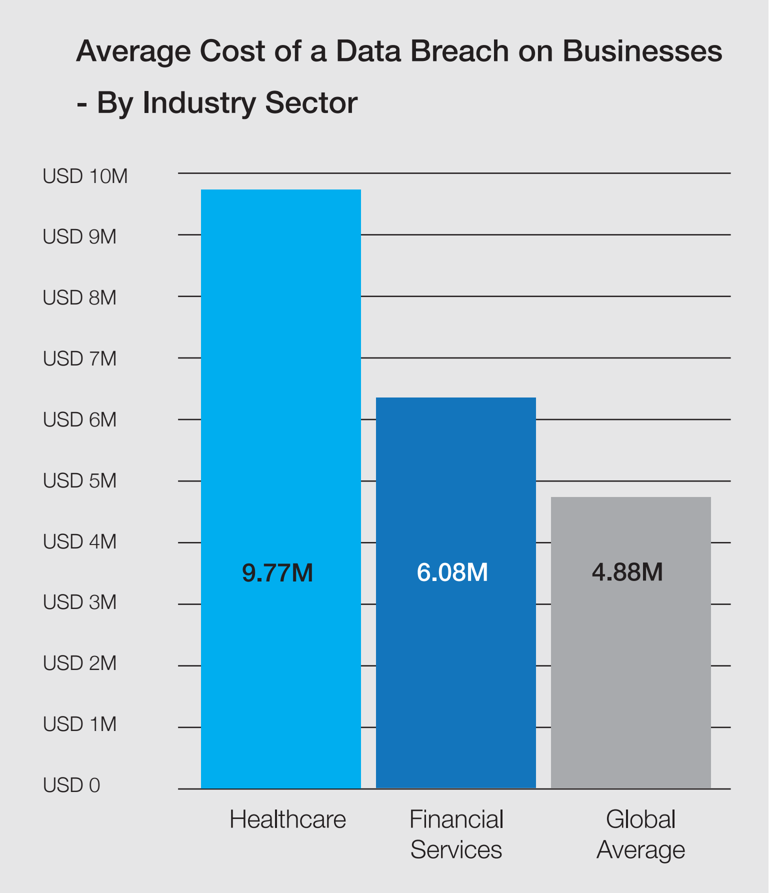
Why Microsoft Alone Isn’t Enough

Microsoft 365 Defender is foundational — but not sufficient:

- **ZAP acts post-delivery**, exposing users [Microsoft DDR 2023]
- **BEC emails are clean** — no malware or links
- Attackers test bypasses using live Microsoft accounts [Gartner 2023]
- Defender depends on user reporting for some threat removals

“Best-in-class AI” means nothing if the threat lands 7 months before it’s flagged.

You need a solution that acts **before the inbox**.



References:
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Sales Claims Don't Stop Breaches. Speed Does.

MailGuard has consistently blocked high-impact threats months ahead of Microsoft and API-based vendors:

- QR-code phishing stopped **7 months earlier**
- Dropbox credential scams blocked **since 2020**
- Microsoft Entra guest-invite attacks stopped on **first encounter**

These weren't anomalies — they were **mass campaigns** targeting CFOs and finance teams.

> *"The risk isn't in the product demo, it's in the delay between innovation and detection."*
>
> **— Craig McDonald, CEO & Founder, MailGuard**

MailGuard —Built to Remove the Exposure Gap

MailGuard was built to fix the inbox exposure gap.

MailGuard delivers:

- **Inline detection before mailbox delivery.** This is where breaches are stopped — not after damage is done, but before users ever see the threat.
- **7-month lead time on emerging phishing patterns** such as QR code phishing attacks
- **Seamless integration** and deployment inline with Microsoft 365 and Google, blocking threats before they reach users.

This is **precision cyber defence at speed**, engineered to intercept threats before human error comes into play.

"I couldn't speak more highly of MailGuard as a reliable service provider."

— IT Manager, Porsche

"The entire implementation process was very simple and easy to manage"

— Help Desk Specialist, Lincraft

"We've seen email-based attacks surge. MailGuard and Defender 365 together have helped us stay protected."

— CISO, Silk Logistics Holdings

Regulatory Pressure Is Rising

Cybersecurity is no longer optional —it's enforced.

Region	Rule	CRO Impact
USA	SEC Cyber Disclosure Rule	Obligation to report material breaches within 4 days (SEC 2024)
Australia	APRA CPS 234	Boards must govern cyber like financial risk
Global	ISO/IEC 27001	Requires email risk controls and audit trails

> *"Companies may be victims of cyber attacks, but must not further victimize investors through misleading disclosures."*
>
> **— Sanjay Wadhwa, SEC Enforcement Director (SEC 2024)**

What Leading CROs Are Doing

- Tracking **Microsoft Miss Rate** as a risk KPI
- Conducting **BEC tabletop exercises quarterly**
- Deploying **pre-delivery interception** layers
- Auditing **email-based payment fraud risk**
- Requiring **email-specific KRIs** in board reports

> *"Every company has at least one employee who will click on anything — and that's hard to protect against."*
>
> **— Brad Smith, President, Microsoft (Microsoft RSA 2021)**

Final Word

Email is your #1 threat vector — because it relies on trust.

Your systems aren't broken. Your people are being manipulated.

And your defences aren't fast enough to stop it.

Boardroom Briefing: 5 Questions Every Board Should Ask

1. What's our detection time for threats that bypass email security?
2. What's our **Microsoft Miss Rate?**
3. Can we **detect BEC with no links or attachments?**
4. Have we **rehearsed incident response under SEC/APRA timelines?**
5. Are we **protecting our people — or just hoping they won't click?**

In a world of AI deception, voice clones, and real-time social engineering…

The inbox is the battlefield.

Make sure you're winning the war.

Built in Australia.
Trusted Globally.

MailGuard is a global leader in email threat detection. A pioneer in cloud email security since 2001, MailGuard invented the concept of pre-filtering email threats before inbox delivery, laying the foundation for the Secure Email Gateway (SEG) category.

Today, MailGuard protects organisations globally with AI-powered threat detection, seamlessly deployed inline with Microsoft's ecosystem and Google, among other email providers.

At the heart of our platform is **MyGuard**, our proprietary AI threat engine developed with over **A$35 million in R&D**. MyGuard combines:

- Gen-AI powered LLMs
- Bayesian and fingerprint-based classifiers
- Real-time behavioural heuristics

…to stop advanced threats on first encounter before they reach staff inboxes — including those that bypass Microsoft and other cloud email security vendors.

MailGuard is **ISO/IEC 27001:2022 certified**, trusted by **over 5,500 organisations**, including governments, law firms, banks, hospitals, and ASX-listed companies. Recognised for our unmatched speed in detecting zero-day email threats, we have consistently stopped sophisticated exploits, like **QR code phishing, Dropbox-based malware**, and **Azure AD Guest Invite fraud**, months ahead of Microsoft, and other leading platforms.

In an era of rising cyber regulation and board-level accountability, MailGuard enhances your Microsoft 365 or Google security stack with minmal disruption, easy activation, and elite-speed protection, fulfilling your fiduciary and operational responsibilities.

mailguard
A GlobalGuard Company

Trusted by Global Leaders.
Since 2001.

- A **leader in advanced 'zero zero-day' email threats** missed by Microsoft 365 and other 3rd party vendors.
- Achieve peace of mind with MailGuard, a solution **trusted by global leaders** that ensures your email is secure.
- Benefit from **A$35M+ in R&D, including proprietary AI & ML-powered threat detection**, to boost your cybersecurity confidence.
- AI-powered email threat detection and inline architecture intercepts and blocks threats hours faster, on first encounter.

"It's the type of innovation that we want to see."

— Satya Nadella, CEO & Chairman, Microsoft

"MailGuard has developed world-leading cloud and email security IP. This is IP that is unique to Australia; it's among the leading cloud and email security solutions anywhere in the world."

— Hon. Malcolm Turnbull, Former Australian Prime Minister

"You are being led by what I see as one of the world's best, at preventing and protecting your secure infrastructure, securing your people, and securing your business"

— Steve Miller, COO, Microsoft Asia

mailguard
A GlobalGuard Company

www.mailguard.com.au

Let’s Connect

Make time today to talk to our local team of experts about fortifying your inboxes.
expert@mailguard.com.au

mailguard
A GlobalGuard Company