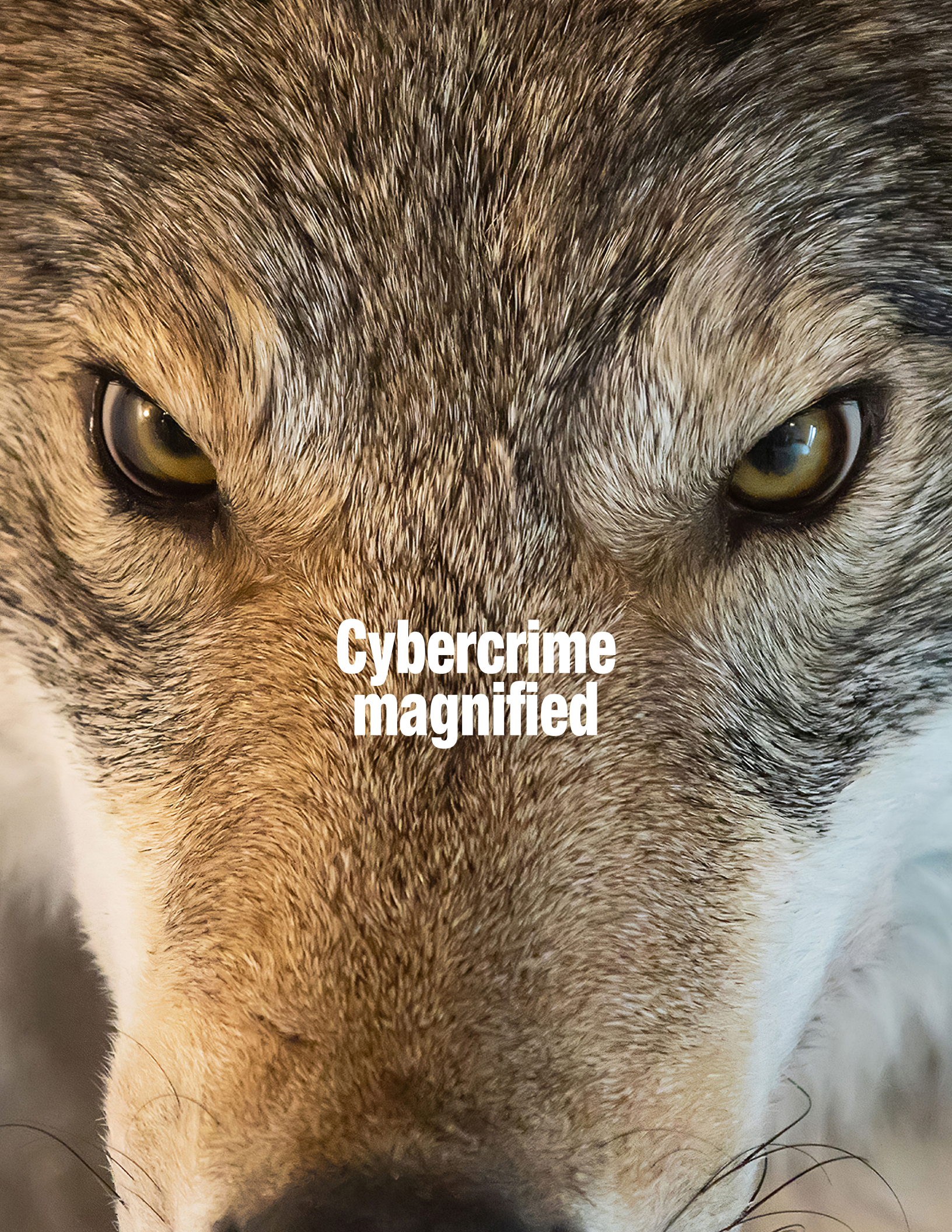

Cybercrime
magnified

Business Email Compromise on AI

Every day brings what can feel like destabilizing changes, including Business Email Compromise (BEC). It's not new, but it has ballooned in its financial consequences – damages are of a size that can easily threaten the survival of a small organization.

But Bryley has observed a rise in BEC attacks that show signs that criminals may be exploiting Large Language Models (LLM) tools like ChatGPT to craft personalized, convincing emails that mimic trusted people.

Here are some examples of how BEC attacks unfold for smaller businesses:

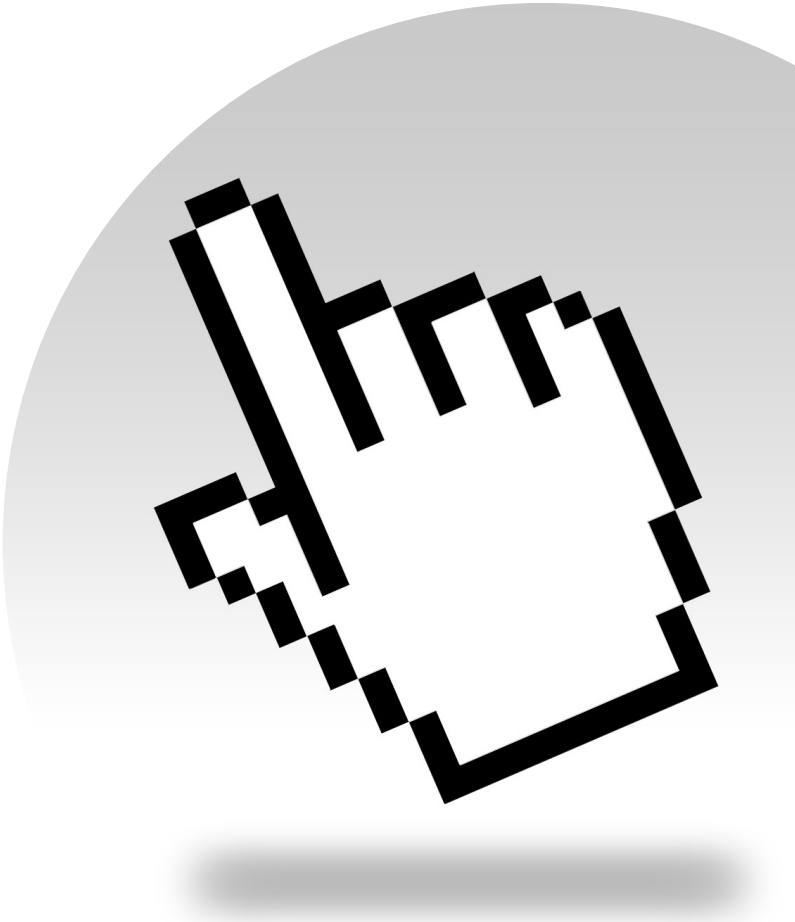
1. A law firm received a Nov. 16 email with instructions to wire $68,403 in payoff funds to a mortgage company. "*That money, instead, went to one of the accounts that [Dwayne] King had opened in Atlanta, authorities said. The next day, [King] withdrew $3,800 in cash from the account at a bank branch, prosecutors said.*"[1]
2. Attackers compromised a Microsoft 365 account, setting up malicious email-forwarding inbox rules to intercept communications to gather a small business' vendor and banking information.[2]
3. A marketing agency invoiced a small business for $103,000, payable via ACH. After the payment was initiated, the business received a suspicious email, supposedly from the agency, claiming suspicious activity and requesting a change of banking details. Thanks to their training, the accounting department verified the request by phone. It was revealed the email was a scam.[3]

The Apple-fication of the web

LLMs fool us. They give us cues that they are, in the words of ChatGPT "clear, concise, and confident" – by design. While their content is nothing new. In fact it's old (some now incorporate an updated search engine's cache of web content). LLMs are pattern finders trained on a lot of data (the web and books) and statistically-based predictors based on those previously seen patterns.

LLMs are like the web with great UI/UX (User Interface/User Experience) design – continuing a trajectory Steve Jobs embraced after his 1979 visit to Xerox PARC, where he saw a computer interface mimicking real life with documents, folders and a desktop. When Jobs returned to lead Apple again in 1997, he doubled down on this idea through skeuomorphism – designing digital elements to resemble real-world counterparts, from page-turning books to metallic window frames. And Apple rose from the dead. Microsoft made a lot of similar interface choices in Windows. Google brought it to Android. Digital design has evolved, but real-world analogies remain; making the digital feel real has long been a human goal. LLMs are a logical and powerful continuation of the evolution of this human-computer interface pursuit.

Below: We've been trained to see these pixels as a hand – now floating via the fake shadow. With effort, the illusion fades. But we've been taught to expect digital interactions to work easily, like they're supposed to. AI-generated BEC attacks exploit this. In mimicking trusted people, criminals play on our expectations of digital predictability. We've had years of being primed to believe illusions that confirm our expectations.



Cover: AI gives criminals the power to scale their operations. As an example, AI can scrape a resource, like freely-available podcast feeds and collect voice samples paired with names of small business owners. And these samples can be processed and made to say 'send money to [a criminally-controlled bank account].'

UI in the emails

LLMs collect data, analyze it and statistically predict the next logical thing.

A criminal trains an AI on collecting your data – squatting as a persistent presence on an employee laptop, silently collecting data over time. It learns communication patterns, internal contacts and financial workflows. An LLM analyzes that data to statistically predict how a specific manager would ask a specific buyer to release confidential data or send money to a criminal account.

Emails have become so convincing employees can't tell them from the real thing. And when the fraud blends seamlessly into the natural workflow – like the hiding wolf – that's when the criminals strike.

Wolves in the grass

AI also lets cybercriminals scale BEC attacks like never before. LLMs can analyze publicly-available data, identify decision-makers and generate personalized emails in seconds – turning once time-consuming scams into mass, automated operations. With AI doing the research, analysis and crafting the emails, even small and mid-sized businesses are sitting ducks.

And traditional security measures were not built for this. AI-fueled attacks can bypass rules-based defenses by not showing the usual give-aways – they can slip past traditional antivirus and anti-malware undetected. Cybercriminals can move broadly and with speed and precision – hitting businesses before the victims even realize there's a threat.

Deep mindset

Just like people are reassessing operations in light of the possible benefits of LLMs, to defend against LLMs' malicious use, also requires rethinking defense. So consider:

- Implementing verification standards: Establish verification protocols for all colleagues, vendors and sensitive requests – especially financial transactions. Familiar communication patterns are able to be exploited in AI-enhanced attacks.
- Cultivating AI Security Awareness Training: Equip your team with up-to-date knowledge of AI's dual role — as both a threat and a defense – and its ability to amplify cybercrime, while providing ongoing training on evolving AI attack techniques and defenses.
- Using AI-powered, adaptive defenses: Deploy intelligent, layered security that can respond dynamically to intelligent attacks.

Above: Small businesses do not have the cybercriminal-fighting resources that larger organizations have. So how should a smaller organization best deal with the growing threats posed by AI?

AI has altered people's interactions with computers, including criminals who are pressing it to see how it can be used to malicious ends. This means AI opens new vulnerabilities – this invites a reassessment of your security strategy.

The changing rules of engagement

The efficiency and sophistication of these AI-driven attacks pose a threat to businesses of all sizes. For the reasons, below, with the introduction of AI, even small organizations are more vulnerable to devastating financial losses.

Bryley has witnessed tactics evolve from ridiculously crude phishing attempts to fake antivirus-update-required emails to sophisticated impersonation scams. At each of these historical moments, the attacks reflected the real-world tech trends of the day. And today we're just in the middle of digital evolution:

1. A small shop receives an email from its owner urging a $75,000 wire transfer to get in on a last-minute bulk order opportunity. Only AI has crafted the email based on scraped social media data, to capture the boss' tone. AI can analyze public profiles to mimic individuals, as pointed out in Huntress's 2023 trend report. And without FTC regulations that demand disclosure by public companies, the FBI reports that when small- to medium-sized businesses are attacked, it might go unreported due to embarrassment or fear of reputational damage.
2. A family-owned bakery is attacked with a deep-fake voicemail from a bank manager insisting on a $50,000 payment to fix an account discrepancy. AI voice synthesis, available on the dark web, makes this possible. A bakery might not report the loss to avoid signaling financial weakness to suppliers.
3. And consider a small law firm where an AI chatbot, posing as a client in a compromised email, tricks a paralegal into transferring $100,000 for a settlement – chatbot tech's conversational skills, highlighted in Microsoft's 2024 Digital Defense Report[4], drives this, and legal firms often hush such breaches to protect client confidence.

Yes, these are hypotheticals, but they aren't far-fetched; they're extensions of documented patterns[5]. But they often go unreported due to shame, financial recovery attempts or client trust concerns.

Limited resources against an enhanced enemy

The fact that smaller operations may have less money to throw at a problem shouldn't be a surprise, but here are ways smaller businesses are particularly affected:

Potential lack of cybersecurity personnel

- no one may be on-site who is expert in cybersecurity
- a limited role is given to an outsourced IT provider often because of budget, instead of involving them to uphold a robust and evolving security stack

Reliance on trust-based relationships

- Larger businesses often have more robust financial controls:
- different people assigned to handle different parts of finances (a built-in checks and balances safeguard)
- better documentation and record-keeping (to trace the movement of funds and detect fraud so they're better able to contain the damage)
- Larger companies usually have a multi-layered approval process, making it more difficult for BEC scams to succeed in the first place. These often include mandatory verification steps for any changes to payment instructions.
- Smaller businesses tend to have less formalized procedures, and so may be more vulnerable to social engineering that exploits personal relationships and trust.

> **Emails so convincing employees can't tell them from the real thing**

The value of what's on the internet

- Larger companies have a generally more sophisticated sales process than small businesses. This makes it likely that smaller businesses will put it all out there – on the web, on social media, etc. (More secure businesses often keep reports behind registration walls.) Readily accessible information makes a prime target for scrapers.
- Small businesses may have less awareness of the risks of web scraping. They might lack dedicated security personnel or the budget for scraping-mitigation approaches.
- A business may underestimate the value of what may seem innocuous information. But it can be used to facilitate a targeted attack (e.g. 'thanks for making the payment change – be seeing you at the Boston show'.

The biggest challenge now

While AI offers appealing up-side, its accessibility also empowers malicious actors with efficient,

scalable attack methods, making any-sized business more vulnerable.

AI-powered cybercrime is revolutionizing BEC scams, enabling criminals to pose as trusted individuals with scale and precision. Using Large Language Models, attackers can now automate the creation of personalized emails and even voice messages by scraping publicly available data like from voices on podcasts or LinkedIn. This lets them bypass traditional security measures and exploit our trust in familiar communication patterns, and so can trick employees into giving away sensitive information or transferring funds to fraudulent accounts.

The availability of AI presents unique and escalating challenges for smaller-sized organizations, who are acutely vulnerable to its misuse in cyberattacks.

Protecting your organization requires a clear understanding of your current security posture and a proactive strategy for mitigating emerging threats. Bryley can help, as they have helped others since 1987.

Contact us at 978•562•6077 or email VP Roy Pacitto at rpacitto@bryley.com to explore building a stronger defense today.

Footnotes

[1] The Patch, Money Laundering Email Scam
[2] Huntress
[3] Huntress
[4] Microsoft's 2024 Digital Defense Report
[5] Microsoft

bryleysystems™

Bryley • Business Continuity through Managed IT

Bryley Systems Inc, 200 Union St, Clinton, MA 01510 • 978.562.6077 • Bryley.com