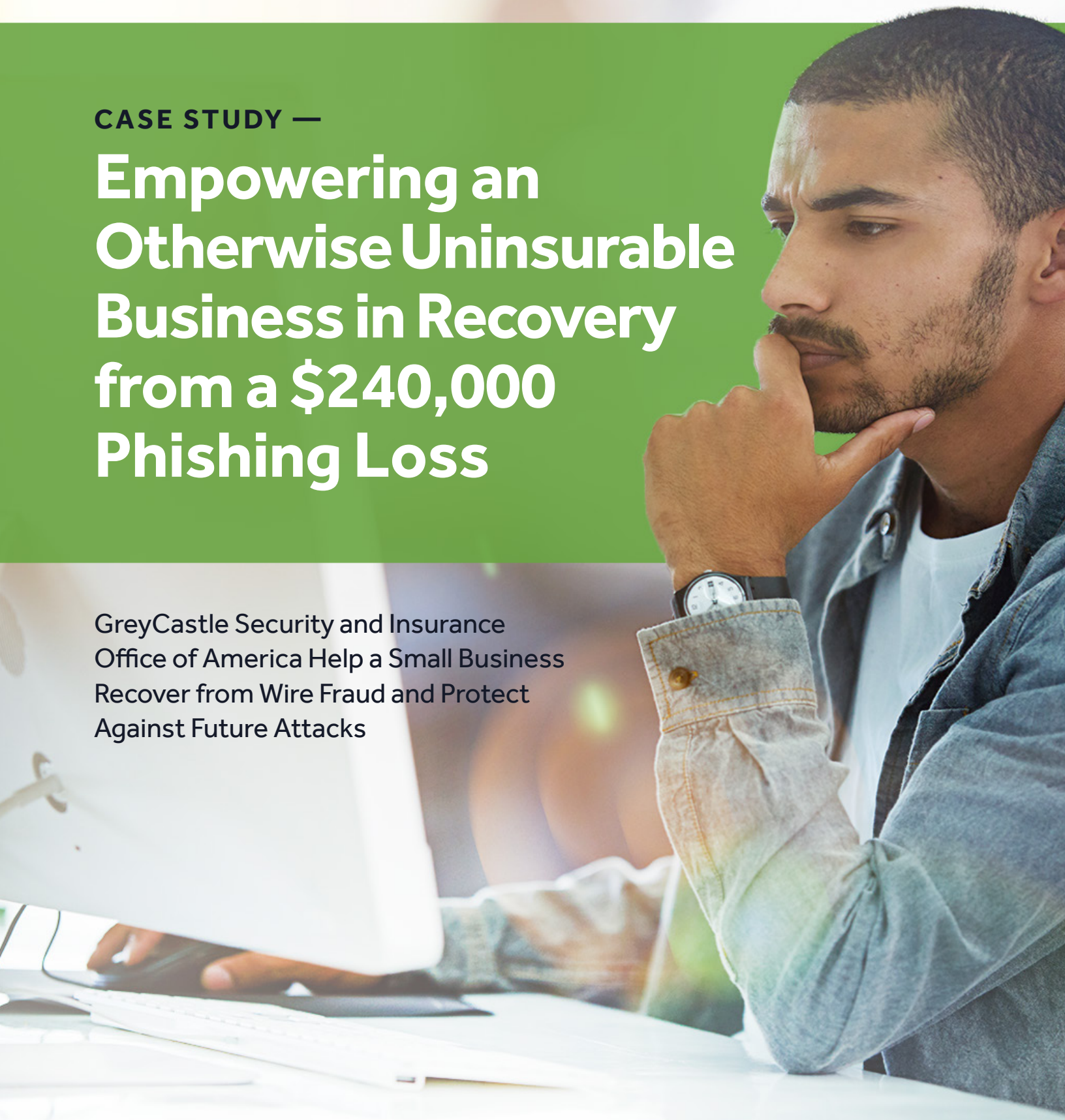
CASE STUDY —

# Empowering an Otherwise Uninsurable Business in Recovery from a $240,000 Phishing Loss



GreyCastle Security and Insurance Office of America Help a Small Business Recover from Wire Fraud and Protect Against Future Attacks

GreyCastle security | IOA INSURANCE OFFICE OF AMERICA

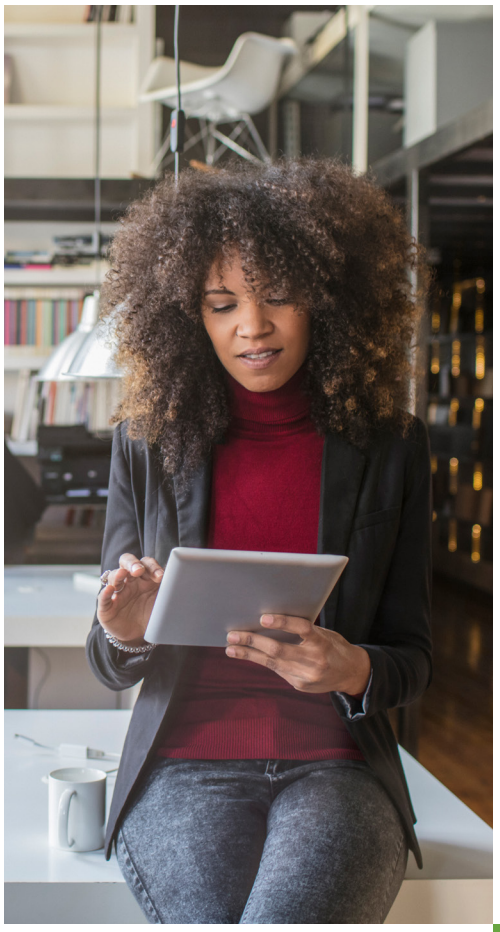
It's all too common; small and mid-sized companies don't realize that every business is a potential target of cyber threats. One company learned the hard way that even small companies are targets, and, if successful, even one cyber event can have a catastrophic effect on your business.

**THIS IS A TRUE STORY. UNDERSTANDABLY, THE COMPANY CHOOSES TO REMAIN ANONYMOUS.**

# BACKGROUND

An employee in a small business received what seemed like a routine email from a known contact, the CFO of a vendor with whom they were already doing business. The employee had received a similar email only weeks prior. The email provided a new bank account to wire funds to for a recent order. The amount for the order was correct—$240,000. The employee updated the account and initiated the transfer of funds. All seemed routine until the vendor contacted the business to notify them the funds had not been received, triggering a review of the transfer.

That initial review uncovered that while the first bank account change request had been legitimate, the second was not. When the company connected with their vendor, it resulted in more questions than answers. How was a fraudulent email sent appearing to be from a legitimate contact with a vendor? Has the business been hacked? Was the company insured against such a loss? Were the funds recoverable?



# OUTREACH FOR ANSWERS

Their current insurance broker was unable to give satisfactory answers or actionable advice. Given the severity of the situation and need for responsiveness, the business's COO reached out to a partner program network and contacted IOA's Jeff Heet, vice president and risk management advisor, who was willing to help in two ways.

First, he reviewed the business's insurance policy. Unfortunately, they were only able to claim $5,000 of the $240,000 lost. Second, he referred the company to GreyCastle Security to help the COO answer his questions about how the wire fraud occurred and how to prevent any additional incidents in the future.

CALL IN THE PROFESSIONALS:

# ENGAGEMENT WITH GREYCASTLE SECURITY

The business was particularly cost-sensitive, especially given their recent loss, but reducing risks and remediating security gaps were top priorities. GreyCastle Security could alleviate some cost concerns by estimating the project would take 10-15 hours, about a third of what other vendors quoted. GreyCastle Security also provided the business with helpful questions to ask other vendors to aid their selection process.

GreyCastle Security's reputation, expertise, and responsiveness along with IOA's endorsement, were the business's deciding factors.

**GreyCastle Security's engagement included three priorities:**

- Conduct an assessment of the email environment to determine which, if any, accounts are at risk.
- Perform forensics on all mailboxes determined to be at risk or compromised.
- Mitigate the risk of incident reoccurrence, as well as future security incidents.

GreyCastle Security quickly reviewed the client's Microsoft 365 email environment and determined that their email system had not been breached. Instead, the breach was on their vendor's end. The telltale clue was a DomainKeys Identified Mail (DKIM) flag in the vendor CFO's email header. It indicated

1. **The vendor CFO's email was not spoofed or forged to appear as though it came from a legitimate address, but rather originated directly from the CFO's email account; and**
2. **The vendor's CFO email account was accessed by an unauthorized actor.**

GreyCastle Security also determined that some simple process changes could have prevented the wire fraud altogether. Specifically, all bank account change requests should be verified by phone or video conference as well as simple electronic communications. This multi-factor identity verification method would have quickly identified the second bank account change as fraudulent. Additionally, if the vendor's email system had also incorporated Multi-factor Authentication (MFA) properly, the hackers would likely not have been capable of accessing their email system.

> **While their vendor was using Microsoft 365, security controls were not implemented; they could have prevented a significant loss.**

Thus, while their vendor was using Microsoft 365, which has email security and logging tools available, a simple procedural misstep caused a significant cybersecurity loss. Because the funds had been transferred internationally and the fraudulent bank account was subsequently closed by the hackers, the $240,000 was not recoverable. However, showing that the breach had occurred on the vendor side paved the way for productive discussions about sharing the loss with their vendor. They avoided an unproductive or contentious back-and-forth. This partnership between our client and their vendor was critical to our client's $4 million business-maintaining operations.

As a best practice, GreyCastle Security recommends implementing multiple layers of security, rather than a single point of failure to prevent, detect, and respond to security events and incidents. Senior Security Specialist Adam Dean shares, "For this particular incident, multiple controls in parallel can be implemented to not only prevent email compromises, but also detect and respond in an efficient and effective manner. For example, the vendor could have implemented MFA, prevented specific email types from being received, and automated behavioral analysis to detect anomalous activity, such as alerting on logins from two locations where the time to travel is impossible. Additionally, the client could have detected this malicious bank account change request by validating the identity of the requesting individual, rather than relying on a single email."

# FROM UNINSURABLE TO INSURED AT A REDUCED RATE

Learning from this experience and unhappy with their prior insurance agency's service, the business again contacted IOA's Jeff Heet for cybersecurity coverage. However, the recent loss made the industry virtually uninsurable without some risk remediation steps. Fortunately, Jeff was happy to provide guidance. First, the company instituted cybersecurity training for its employees, including how to spot fraudulent emails, use MFA for applications including email, and use multiple identity verification steps to verify bank account changes.

The business's newly instituted ongoing training combined with following through on GreyCastle Security's security recommendations resulted in the organization not only qualifying for cybersecurity insurance but also qualifying at a 50% reduced rate from previous quotes.

> **"Any company with email needs cybersecurity insurance, period."**

Cybersecurity insurance and a strong cybersecurity program are so important whether you're protecting funds, like this client, or safeguarding confidential, protected information. Jeff states, "Any company with email needs cybersecurity insurance, period." And every policy will be different depending on the type of business and level of risk. In this case, as with many businesses, social engineering will be an ongoing risk, and that's where the cybersecurity training helps lower a company's risk and insurance rates. Still, there's always a chance an employee gets busy and cuts corners or inadvertently clicks on a malicious link. Any cybersecurity breach has financial and reputational consequences, and that's what cybersecurity insurance is for."

# BENEFITS OF WORKING WITH PARTNERS

While the business did suffer some financial loss due to this incident, its partnerships with GreyCastle Security and IOA helped leadership determine the cause of the incident. Together, the IOA and GreyCastle Security team enabled their client to:

1. **Mitigate their active risks,**
2. **Decrease their risks of future cyberattacks,**
3. **Protect themselves from future losses and expenses like higher insurance rates, and**
4. **Find peace of mind with cyber insurance they were previously unable to obtain.**

# LESSONS LEARNED

- Use Multi-Factor Authentication for all applications, tools, and business processes where possible.
- Confirm any financial changes including banking, payroll, and invoicing through a minimum of two forms of confirmation: digital and personal confirmation.
- Develop and maintain a security program outside your organization to ensure it is active, managed, and audited periodically.
- Ongoing employee security training to enable your organization to spot, communicate, and mitigate suspicious activity and potential threats.
- Conduct risk assessments on your entire business, including vendors, to provide helpful context to make business decisions.
- Maintain cybersecurity insurance coverage adequate for your business risks, including situations where the breach occurs with a third party like your vendor or partner.

## ABOUT INSURANCE OFFICE OF AMERICA

Insurance Office of America is a full-service insurance agency founded in 1988, and it is one of the fastest-growing independent agencies in the United States. IOA has more than 1,300 associates located in over 60 locations in the U.S. and Ireland.

---

## ABOUT GREYCASTLE SECURITY

GreyCastle Security was founded almost a decade ago on the principle that cybersecurity and effective defense is entirely possible if you use common sense, apply a system of measurement, and know what you're trying to protect.

We help organizations to develop effective cybersecurity programs, minimize the impact of state and federal compliance regulations, improve client retention, and mitigate security incidents. Our revolutionary approach to service delivery solidifies the business mindset that cybersecurity is not just an "IT" issue – it's about the overall health of your business.

For more information, visit **www.greycastlesecurity.com.**