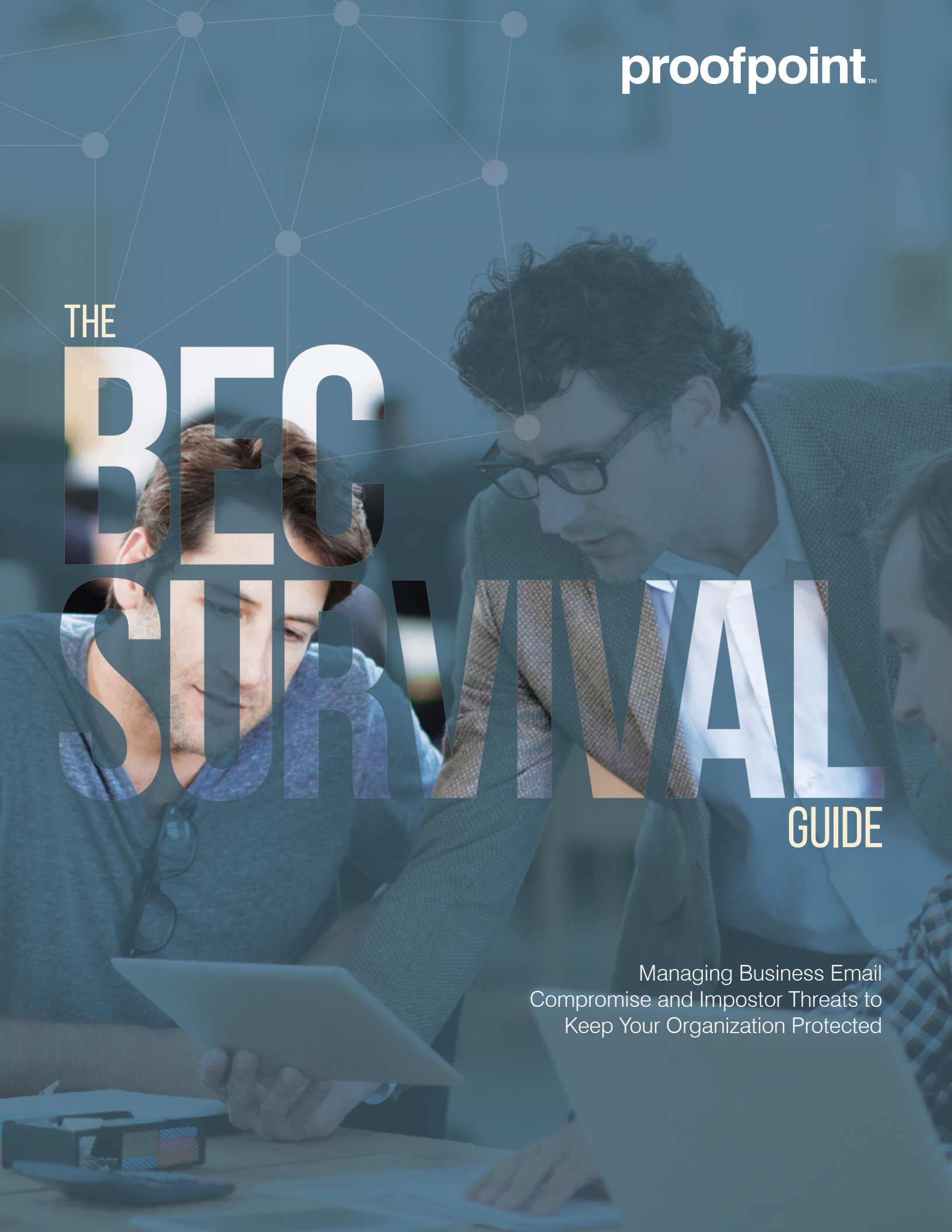
proofpoint™

# THE BEC SURVIVAL GUIDE

Managing Business Email Compromise and Impostor Threats to Keep Your Organization Protected



# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

Business email compromise (BEC) is a simple attack that is confounding some of the most advanced companies in the world.

Since the FBI began tracking BEC attacks in 2015, more than 22,000 organizations worldwide have fallen victim to them, losing an estimated $3.08 billion.[1]

Unlike other cyber attacks, BEC emails don't contain malware or malicious URLs. Instead, they take advantage of social engineering.

BEC attacks target people—usually your CFO or people in your human resources, finance, or payroll departments. Using a technique called "spoofing", the attacks trick your people into thinking they've received an email from a boss, co-worker, vendor, or partner. The impostor requests wire transfers, tax records, and other sensitive data.

BEC attackers succeed because they create emails that are deceptively similar to legitimate messages. They also ask victims to perform tasks that fall under their normal job duties.

This very simplicity enables these emails to slip by traditional security solutions designed to detect attacks that exploit technology.

**How to Protect Your Organization**

Fortunately, you can stop BEC attacks though a combination of people, process and technology.

*Before an attack*

You can avoid BEC attacks with a three-pronged approach:

- BEC awareness training for staff.
- Procedures and policies for business processes conducted via email.
- Advanced threat protection that blocks BEC attacks before they reach employees' inboxes. This protection should also block your employees from divulging sensitive information if they are tricked into communicating with BEC attackers.

An effective solution combines two powerful capabilities. It detects and stops BEC at your email gateway. And it authenticates your organization's emails as at the gateways of your partners and the consumer email providers you customers use.

Consider using the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication Reporting & Conformance (DMARC) in this effort. In addition, consider data loss prevention (DLP) controls on your email gateway. This step will protect the types of sensitive information BEC attackers are likely trying to get.

[1] FBI. "Business E-Mail Compromise: The 3.1 Billion Dollar Scam." June 2016.

### *After an attack*

Cyber criminals are always looking for new ways to trick your people, evade your technology and profit from the experience.

If a wire-transfer attack was successful, start the recovery process by contacting your bank. Ask it to contact the bank where the transfer was sent. Then contact your local law enforcement and report the attack.

You may also need to notify your insurers and shareholders. And if sensitive information has ended up in the hands of cyber criminals, you'll need to mitigate the fallout.

Assessing why the attack was successful is also important. No matter what the cause of the attack, revisit your training efforts to update people on the threat landscape, the anatomy of the attack and new solutions.

Although BEC attacks don't rely on malware, a successful attack may point to weaknesses in your cyber defenses. Consider a threat assessment to discover any hidden risks and gauge your readiness to respond to future threats.

### *Keys to a strong defense*

BEC attacks are a growing threat to businesses because they prey on vulnerabilities that can't be patched: people. That's why employee training, financial controls, and technology are the keys to a strong defense and effective response.

You need a solution that does not solely depend on reputation and basic email configurations. With granular controls, advanced email solutions can identify and quarantine impostor emails before they reach your employees' inbox.

# INTRODUCTION

# A GROWING PROBLEM

Falling for an impostor's email is easier than you might think. Imagine this scenario: You work for a large company that has been involved in acquisitions. Your job is to pay the bills. One morning, you get an email from your CEO who's travelling. He wants you to do a wire transfer so that he can start the process of acquiring another company. And he doesn't want you to tell anyone until the deal is done.

It's not uncommon for your CEO to email you about wiring money. And it makes sense that he doesn't want the news to leak.

Another situation: Your company has a foreign supplier. You've heard that the supplier is making some changes to its operation. An email comes to you from the supplier: "We are changing banks." The email directs you to send all future payments to the new bank and provides the account information.

The supplier's name is real. The sender's name is real. The bank is real.

But in both scenarios—taken from real-life cases—the email is a scam. They're examples of business email compromise (BEC), an attack that has hit more than 22,000 organizations around the world and cost an estimated $3.08 billion since the FBI began tracking it in January 2015.[2]

BEC attacks use email to trick people into wiring money or sending sensitive corporate information such as employees' personal data.

From the appropriate person, requests for wire transfers or sensitive employee information can be legitimate. They're received by companies around the world every day. They make modern business possible. The trouble is, telling the difference between authentic emails and a BEC impostor scam is not always easy. And a case of mistaken identity can be costly.

Fortunately, you can prevent BEC attacks from succeeding. Consider this guide a starting point. We'll reveal the factors behind the surge of BEC attacks, what to do if it happens to you, and most important, how to avoid falling victim in the first place.

[2] FBI. "Business E-Mail Compromise: The 3.1 Billion Dollar Scam." June 2016.


# HOW BEC WORKS: TARGETS AND TACTICS

Your people are your strongest asset. But when it comes to cybersecurity, they can also be your weakest link. They're vulnerable to attacks that exploit human nature, not just technical flaws.

Cyber criminals research their victims to find the best people within the organization to target. They'll study your organization and become a frequent visitor to your website. They'll go on social media sites such as LinkedIn to learn about your people—their title, where they've worked, people they've worked with, and their interests.

# TARGETS

If cyber criminals want to steal money, they'll learn about your people in finance. About 47% of impostor emails target CFOs.[3] If they want sensitive corporate or personal employee information, they'll find out all they can about your human resources (HR) people. About 25% of attacks target HR.[4]

They'll look for new employees who may not be familiar with your organization's policies and procedures. They'll note when your top executives travel, and where, and keep a record of your organization's busiest times during the day and week. It's all to make their spoofed messages appear as real as possible and take advantage of windows of opportunity to profit.

# TACTICS

BEC attacks target people. The attacks are designed to trick your people into thinking they've received an email from a high-level executive in your organization such as the CEO or a supplier, partner or co-worker. The sender of the spoofing or imitation email requests action such as wiring money or providing tax records or other sensitive corporate or personal data.

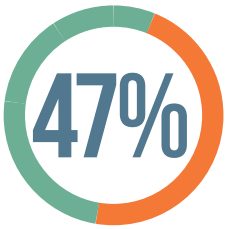
At a quick glance, nothing about the email seems out of the ordinary. But slight differences— such as in the sender's name, sender's address, or the reply address—are telltale signs of an impostor. The cyber criminals count on their target not taking the time to verify the email.

[3 & 4] Proofpoint research. March 2016.

## WHO'S BEING TARGETED

Here's a breakdown of employees and departments targeted in BEC attacks.


**Chief Operating Officer**




**Chief Financial Officer**


**Human Resources**


**Finance**


**Payroll**

Source: Proofpoint

# THE MANY FORMS OF BEC

Here are the four most common variations of BEC emails:

75%

### Spoofed Name

This variation represents 75% of attacks. It uses the name of the spoofed executive in the "From" field. But the email address comes from an outside service such as Gmail that belongs to the attacker.

21%

### Reply-To Spoofing

This technique uses the real name and email address of the sender being impersonated (typically the CEO). The "Reply-to" name also uses the name of the impersonated sender. But the Reply-to address—where any replies are sent—is the attacker's.


2%

### Spoofed Sender (with No Reply-to Address)

This form of BEC email uses the name and email address of the spoofed executive. But the email does not contain a "Reply-to address," so two-way correspondence is impossible. The email often includes wire-transfer instructions to make follow-up messages unnecessary.

2%

### Lookalike Domain

In this form of BEC attacks, the attacker's "From" address is similar in appearance to the impersonated executive's address. The lookalike domain could be just one letter off from the real one: "**legt**company.com" for "**legit**company.com," for example.

Source: Proofpoint

# WHY BEC SUCCEEDS

The BEC business is a lot like the Hollywood blockbuster model. Most attempts will flop. But the few that do succeed can yield spectacular returns.

For cyber criminals, the difference between a hit and a miss can hinge on how well they research an organization, target the right people, and time the delivery of their spoofed emails.

In addition to imitating the look of a legitimate email, cyber criminals use proven psychological tricks. They play on the eagerness of workers to please leaders, creating a false sense of urgency and demanding secrecy. To avoid suspicion, the attackers ask victims to perform tasks that the victims do every day for their work.

Spoofing emails often arrive when decision-makers are out of the office, making them difficult to verify. Or they come during busy times, when victims are likely juggling tasks and less vigilant about BEC threats.

BEC emails are a challenge because unlike other cyber attacks, they don't contain malware attachments or malicious URLs. Instead, cyber criminals use social engineering. And that means impostor emails can slip by traditional security solutions that focus on malicious content or behavior that exploits technological weaknesses.

For cyber criminals, BEC attacks offer a low-risk, high-return opportunity. They don't require costly infrastructure. And because attacks often cross international borders, few scammers are prosecuted.

# RECENT BEC ATTACKS

Here's a sampling of documented BEC attacks.

### FACC AG (reported January 2016)

Cyber criminals using a BEC attack stole USD $55.7 million from the Austrian engineering firm that designs and manufactures aircraft components. The company's CEO and CFO were fired as a result of the attack.

### Crelan (reported January 2016)

After an internal audit, the Belgian bank discovered it had lost more than USD $70 million due to imposter emails.

A Crelan bank branch in the Netherlands.

### TWoA (reported December 2015)

A New Zealand college lost more than USD $100,000 when the CFO fell victim to an impostor email that requested payment.

### Ubiquiti Networks, Inc. (reported August 2015)

The provider of high-end wireless networking products paid nearly USD $47 million to attackers posing as a supplier.

### Luminant Corp. (reported 2013)

The Texas electric utility company sent more than USD $98,000 in response to an email with a fraudulent domain name.

# PROTECTING YOUR ORGANIZATION

The good news: you can stop BEC attacks before they succeed. The best defense combines people, process and technology—you need all three.

# BEFORE AN ATTACK: PREPARE AND PREVENT

Training can help your people recognize the signs of an impostor email and follow best practices to avoid falling for BEC attacks. Employing the right procedures and policies can help guide your people in safely handling email requests. And the right technology is essential for detecting and stopping attacks before they reach your people.

### Training

Security awareness training about BEC attacks and cybersecurity in general can help your organization avoid attacks and minimize the effects of an attack that succeeds. The more your people know, the better the chance for a strong defense.

Training should cover the threat landscape, the latest social engineering techniques, and how to spot impostor emails. Make sure your people know your organization's normal operating procedures and policies for how executives, partners and customers request funds and sensitive data.

If possible, include in your training details of actual BEC attacks to show how attack strategies play out in the real world.

### Process

BEC attacks are socially engineered to trick people, so they're designed to be believable. Even the best employees can fall for a well-crafted, well-executed BEC scam. That's why a clear, rigorous process for handling and scrutinizing email requests can provide a critical check against deceptive email requests.

The FBI suggests creating rules that flag emails with extensions that are deceptively similar to your corporate email. Registering domains that vary slightly from your organization's actual domain can stop criminals from using those variants to fool your people.[5]

Consider implementing internal finance and purchasing controls featuring a two-step (or more) verification process. Controls could include requiring more than one person for authorization, written approvals for large amounts and confirmation by telephone. When employing phone verification as part of a two-step process, use previously known numbers—not the numbers provided in the email request.

According to the FBI, some financial institutions have delayed processing customer requests for international wire transfers to verify the legitimacy of the requests.[6]

[5] FBI. "Business Email Compromise." August 2015.
[6] FBI. "Business E-Mail Compromise: The 3.1 Billion Dollar Scam." June 2016.

# SEVEN TIPS FOR HANDLING A SUSPICIOUS EMAIL

### TIP 1: DON'T TRUST THE DISPLAY NAME

A favorite tactic with cyber criminals is to spoof an email's display name. Always check the email address in the "From" header.

### TIP 2: DON'T TRUST THE HEADER FROM THE EMAIL ADDRESS

Cyber criminals not only spoof brands in the display name but also spoof brands in the header from the email address, including the domain name. Make sure everything's correct. If you're suspicious, confirm the authenticity of the message with the person who supposedly sent it.

### TIP 3: CHECK FOR SPELLING MISTAKES

Legitimate messages usually don't have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

### TIP 4: BE CAUTIOUS ABOUT HIGH-LEVEL EXECUTIVES REQUESTING UNUSUAL INFORMATION

How many CEOs want to review tax information for individual employees? How often does your CEO get locked out and require access to your network or needs a password?

### TIP 5: THINK ABOUT URGENT REQUESTS

Is there a good reason for that action? Invoking a sense of urgency and secrecy—especially when bypassing normal channels—are common tactics with BEC attacks. Again, confirm the authenticity of the message with the person who supposedly sent it.

### TIP 6: REVIEW THE SIGNATURE

Lack of details about the signer or how you can contact a company strongly suggests a BEC attack. Legitimate businesses provide contact details.

### TIP 7: DON'T BELIEVE EVERYTHING YOU SEE

Cyber criminals are extremely good at what they do. Many fraudulent emails include convincing brand logos, language and a seemingly valid email address. Be skeptical when it comes to your email messages.

**Technology**

A comprehensive technology solution is the third, and arguably most important, pillar of a strong BEC defense.

Your solution should support advanced configuration options for flagging suspicious messages based on attributes such as direction and subject line.

It should also be able to detect and classify BEC threats at the email gateway. One proven detection method is dynamic classification. This approach employs dynamic and algorithmic approaches to examine the sender-recipient relationship, domain reputation and other attributes. It can catch multiple types of BEC attacks, even as they change.

An effective solution also includes proactive authentication or policy-based protection for your people, partners, vendors and customers. As BEC attacks increasingly target partners and vendors beyond your own email gateway, your organization should provide a way to verify that emails are coming from you and not a fraudster. Two email authentication technologies can help to identify the sender of a message: Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM).

SPF specifies who can send an email on behalf of a domain. It lists IPs of authorized senders in a DNS record. If the IP sending email is not listed in the SPF record, the message fails authentication.

DKIM, meanwhile, makes it possible to transmit a message in a way that can be verified by the email provider. Emails can be digitally signed from a specified domain. Verification is made possible through cryptographic authentication within the digital signature of the email.

A newer authentication tool called Domain-based Message Authentication Reporting & Conformance (DMARC) enhances the protection provided by SPF and DKIM. DMARC is an open email technology that authenticates legitimate senders and extends security to partners and consumers. Among global consumer mailboxes, 85% are DMARC-enabled.

Each of the authentication technologies has its pros and cons. But working in conjunction with your enterprise cybersecurity infrastructure, the combined approaches can filter out a wide range of BEC attacks.

## THE BENEFITS OF DMARC

A DMARC policy allows senders to indicate that their messages are protected by SPF, DKIM, or both. DMARC tells a receiver what to do if neither of those authentication methods passes— such as move the message to a junk folder or reject it entirely.

### DMARC EMPOWERS SENDERS TO:

- Gain visibility into who is sending on your behalf, what email is authenticating, what email is not, and why
- Instruct email receivers on how to handle mail that doesn't pass authentication
- Block attacks spoofing owned domains before they reach employee and consumer inboxes

### DMARC EMPOWERS RECEIVERS TO:

- Distinguish between legitimate senders and malicious senders
- Foster consumer loyalty and employee protection
- Improve and protect the reputation of the email channel

# AFTER AN ATTACK

The best BEC strategy is to avoid it in the first place. But cyber criminals are always looking for new ways to trick your people, evade your technology, and profit from the experience.

Unlike most other cyber threats, BEC attacks don't involve malware or take up residency in your system, so there's nothing to eliminate. But the financial impact can be long-lasting.

If the attacker has stolen money, organizations often make an immediate move for recovery; however, the effort rarely succeeds. In the case of Ubiquiti (see page 14), the company was able to recover only a small portion of the nearly USD $47 million stolen.[7]

Other immediate steps include documenting and reporting the attack—regardless of the size of the loss or timing. If the attack is recent, the FBI advises organizations to contact one of the agency's local offices. The agency works with the U.S. Department of Treasury Financial Crimes Enforcement Network to help return or freeze funds.

When reporting a BEC crime, the agency recommends including the following information to assist with possible recovery:

- Originating name, location, bank name and bank account number
- Recipient name, bank name, account number, location (if available) and intermediary bank name (if available)
- SWIFT number, date, amount of transaction and any additional information such as For Further Credit (FFC)

You should also notify your insurers and shareholders, if applicable, and conduct damage control. For example, if sensitive information has been sent, you should mitigate the risks of it being misused. For stolen tax information, consider providing affected employees with identity theft protection.

Assessing why the attack was successful is also important. Are your current cybersecurity tools up to the task of protecting against BEC and other threats? Where are the holes? Consider a threat assessment to discover hidden risks.

No matter what the cause, it's usually a good idea to revisit your training efforts to update people on the threat landscape, the anatomy of the attack and new solutions.

### Reporting a BEC Attack

Many countries have government organizations that cover cyber fraud, including BEC attacks. Here are a few:

- United States – FBI's Internet Crime Complaint Center (www.IC3.gov)
- Canada – Canadian Anti-Fraud Centre/Centre Antifraude du Canada (www.antifraudcentre.ca)
- UK - Action Fraud (www.actionfraud.police.uk)
- Australia Australian Cybercrime Online Reporting Network (www.acorn.gov.au)
- Singapore – Singapore Computer Emergency Response Team (www.csa.gov.sg/singcert)
- Netherlands - Fraud Helpdesk (www.fraudhelpdesk.org)
- Germany - German Federal Criminal Police Office (BKA) (www.bka.de)

[7] Krebs on Security. "Tech Firm Ubiquiti Suffers $46M Cyberheist." August 2015.

# CONCLUSION AND RECOMMENDATIONS

BEC attacks are a growing threat to businesses because they prey on vulnerabilities that can't be patched: people. That's why employee training, financial controls, and especially technology are the keys to a strong defense and timely response.

You need need a solution that does not solely depend on reputation and basic email filtering. With granular controls, advanced email solutions can identify and quarantine impostor emails before they reach an employee's inbox.

**To learn more about BEC attacks and how Proofpoint can help you safeguard your organization, visit www.proofpoint.com.**

# BUSINESS EMAIL COMPROMISE SURVIVAL CHECKLIST

Here's a quick checklist to access whether you're ready to prevent and manage BEC and impostor threats or not.

## Before an Attack: Preventing

- ☐ **Train your people on security awareness**
  - ☐ Threat landscape
  - ☐ Latest social engineering techniques
  - ☐ Identifying impostor emails
  - ☐ Executive, partner and customer habits regarding requests
- ☐ **Develop a clear, definite process for handling and scrutinizing emails**
  - ☐ Rules to flag emails with extensions that may be deceptively similar to your corporate email
  - ☐ Lookalike domain registration—before criminals do it
  - ☐ Internal finance and purchasing controls with a two-step or more verification process
    - ☐ More than one person for authorization
    - ☐ Written approvals for large amounts
    - ☐ Confirmation by telephone
    - ☐ Delayed processing to verify legitimacy
- ☐ **Implement a comprehensive technology solution**
  - ☐ Advanced configuration options for flagging suspicious messages based on attributes
  - ☐ Detection and classification of BEC threats at the email gateway
  - ☐ Proactive authentication or policy-based protection for your people, partners, vendors and customers—SPF, DKIM and DMARC

## After an Attack: Recovery and Getting Back to Business

- ☐ **Contact your financial institution**
- ☐ **Request your financial institution contact the institution where the transfer was sent**
- ☐ **Contact your local law enforcement**
- ☐ **Conduct damage control**
- ☐ **Assess why the attack was successful**
- ☐ **Revisit training**
- ☐ **Reassess your security posture. Do your email security tools**
  - ☐ Detect and classify BEC emails at the gateway?
  - ☐ Provide proactive authentication or policy-based protection?
  - ☐ Use SPF, DKIM, and DMARC?

## ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint™ www.proofpoint.com