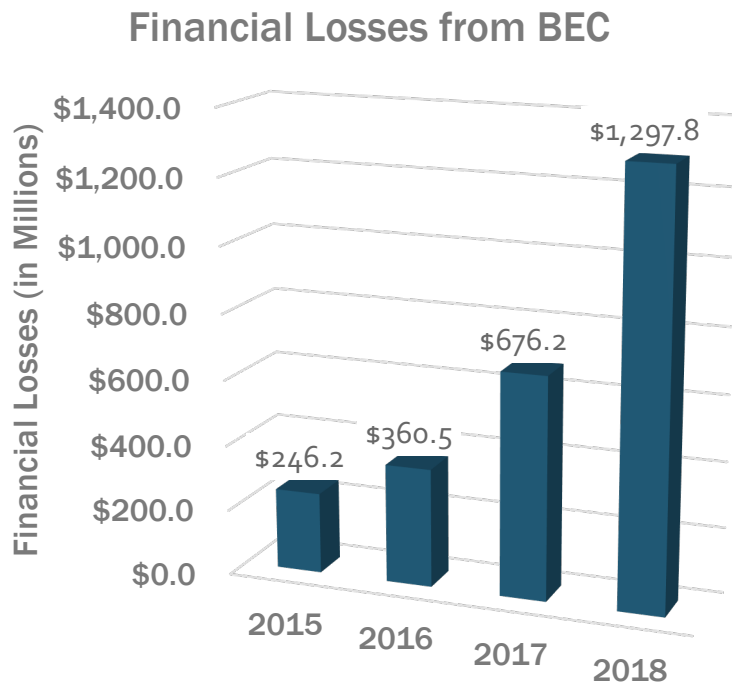




June 3, 2019

3 Reasons Your Email Security is Failing – And How to Fix It

By The Numbers: Financial Losses from BEC



- > 427% increase in financial losses since 2015
- > 48% of financial losses in 2018 due to BEC
- > More than \$3B spent to prevent in 2018

Source: FBI

Businesses at Risk: A Flawed Approach

Despite
EMAIL SECURITY,
detection is failing



Email security tools fail to catch impersonations in

64%

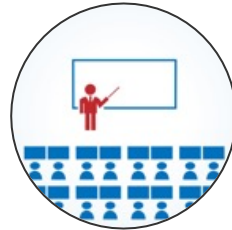
of organizations

Businesses at Risk: A Flawed Approach

Despite
EMAIL SECURITY,
detection is failing



Despite
TRAINING,
users still engage with phish



50%

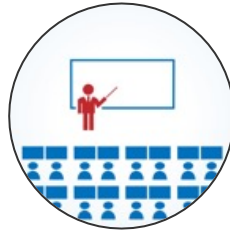
of professionals cannot differentiate advanced email threats from spam

Businesses at Risk: A Flawed Approach

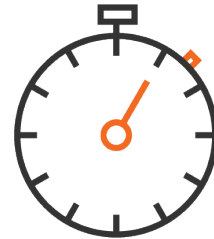
Despite
EMAIL SECURITY,
detection is failing



Despite
TRAINING,
users still engage with phish



Despite
TOOLS & STAFFING,
IR is frequent / time-consuming

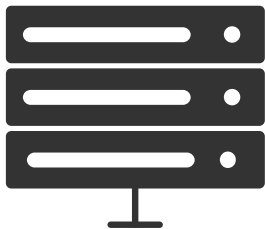


1 in 5
security professionals have to take direct remediation action at least
weekly



3 Reasons Why Email Security Isn't Working

Reason 1: Security Paradigm Shift



LEGACY APPROACH

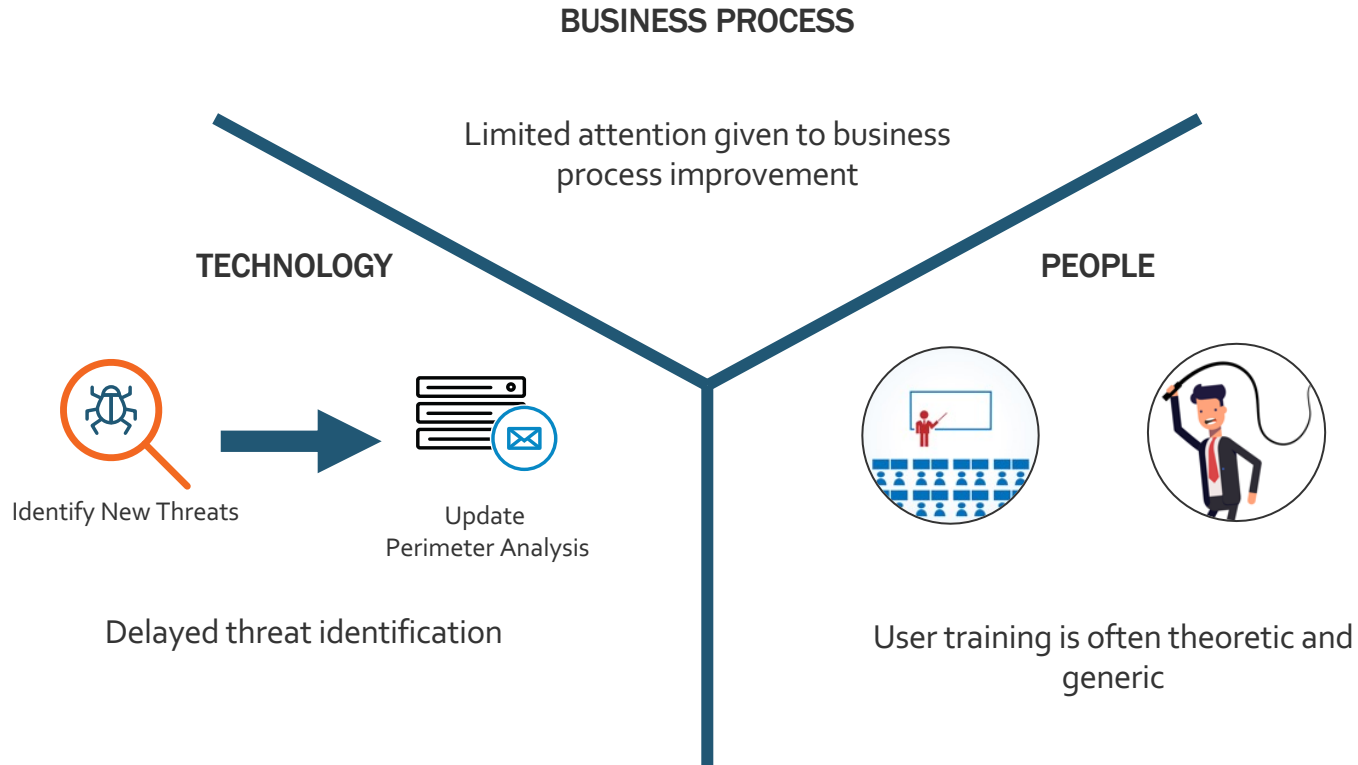
Binary, Intrusive, Event-Driven



CLOUD ARCHITECTURES

Continuous, Adapted to Organization,
Supports Business Operations

Reason 2: Over-Reliance on Technology as a Panacea



Reason 3: Technology Can't Keep Up

DELAYED THREAT IDENTIFICATION



CURRENT APPROACH



Generic, "black box" threat detection



"Single point of failure" detection



Adversarial approach –
"users are the weakest link"

WHAT COMPANIES NEED



Adaptive threat detection



Continuous risk and response



People-centric security –
"users are the best source of intelligence"

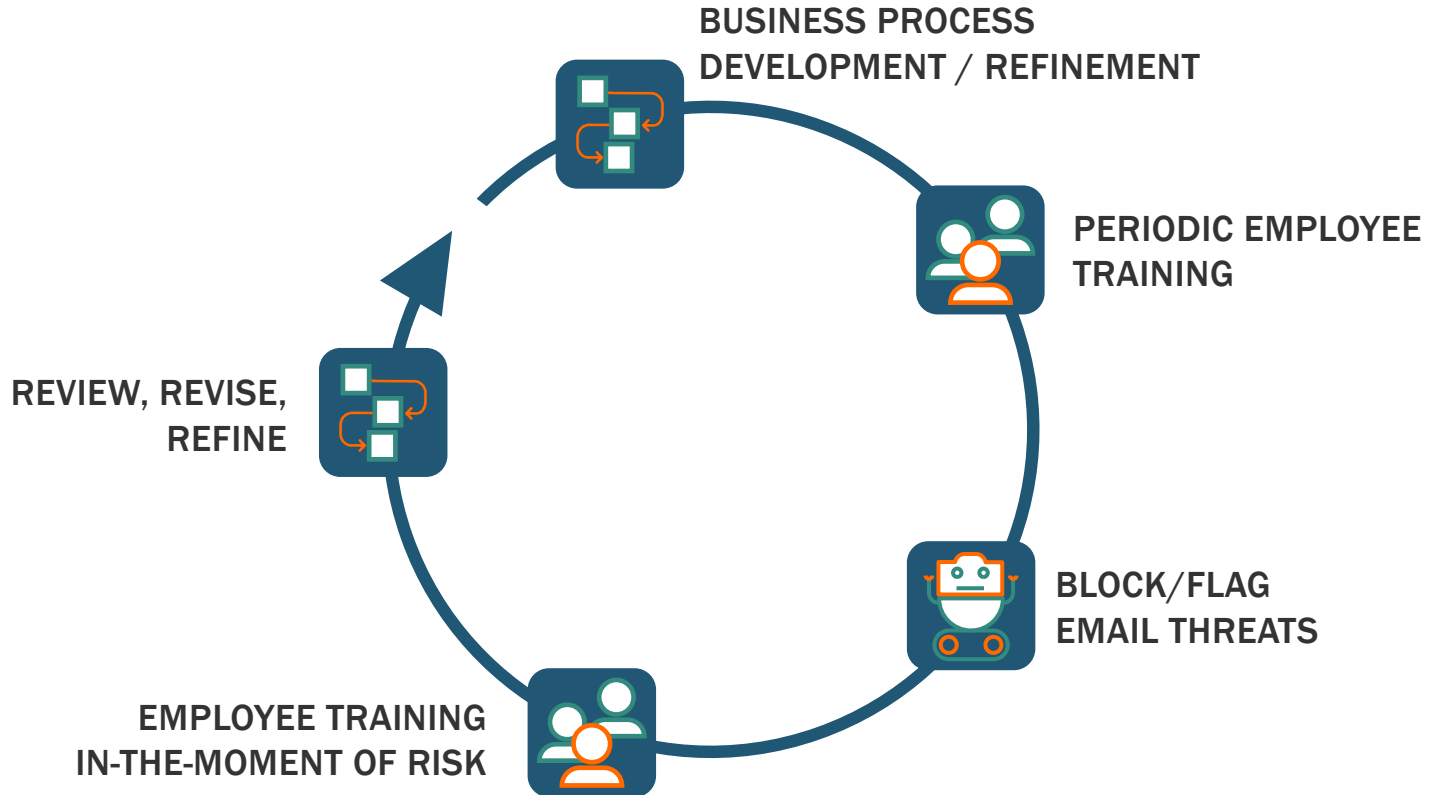


So How Do We Fix It?



Idea 1: Adaptive Risk & Response

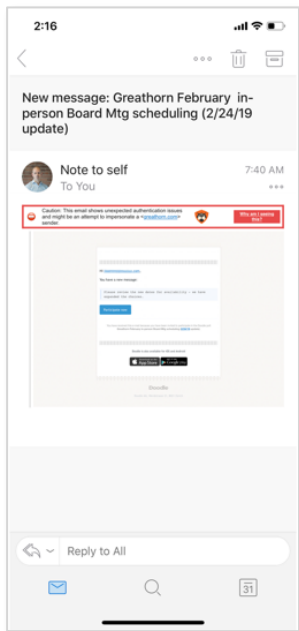
Align Email Security with Cloud's Continuous Improvement Cycle







Idea 2: People-Centric Security

Training in-the-Moment of Risk

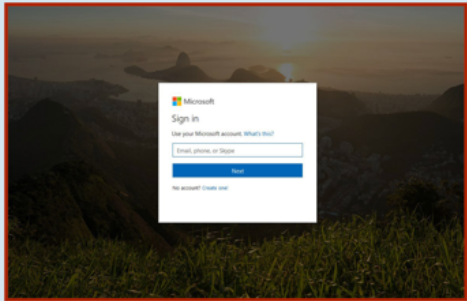


 Caution - this is not the email address that Sherry McWilliams typically uses! This may be an impersonation attempt.

Why am I seeing this?

 **CREDENTIAL THEFT SITE DETECTED**

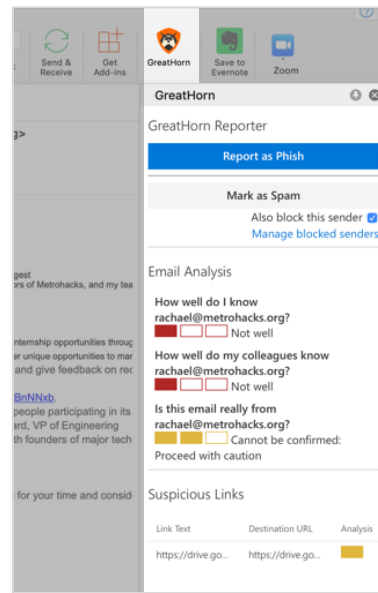
DESTINATION PAGE PREVIEW



Why am I seeing this?
The link you clicked on is an attempt to steal sensitive information, such as your username or password. The link is impersonating Office 365.
For your protection, access to this page has been automatically restricted.

What should I do?
You may safely close this browser window. No further action is required.
If you believe this website is legitimate, click the "Report as safe" button to request access to the website. The security team will review your request.

[Request Review](#)



GreatHorn Reporter

[Report as Phish](#)

[Mark as Spam](#)
Also block this sender
[Manage blocked senders](#)

Email Analysis

How well do I know rachael@metrohacks.org?
■ ■ ■ Not well

How well do my colleagues know rachael@metrohacks.org?
■ ■ ■ Not well

Is this email really from rachael@metrohacks.org?
■ ■ ■ Cannot be confirmed:
Proceed with caution

Suspicious Links

Link Text	Destination URL	Analysis
https://drive.go...	https://drive.go...	■

“

In a clear way, we explain at the exact moment when an employee could engage with a phishing email, that this message could be a *real* attack. We help them better understand the signs.

JEFF KOHRMAN
HEAD OF GLOBAL SECURITY

Hi there,

Our automated security platform (GreatHorn) just spotted an email in your inbox that looks like a W2 phishing attempt.

The email was from " [REDACTED] ", with a subject line of " **RE: [REDACTED]** ", and it was sent with a timestamp of " **Wed Apr 17 2019** ". Just to be safe, we've moved it to a folder in your email called "**Possible Phishing**"; please be careful when reviewing it!

Did we miss a phishing email? Forward it to [REDACTED]!

If you have any questions or comments, please let us know at [REDACTED]

Thanks!
The IT & Security Team



“

We now know what kinds of information our employees are being asked to provide and which users are at the highest risk, and we can tie that back to our business processes and training to reduce risk even further.

JEFF KOHRMAN
HEAD OF GLOBAL SECURITY



Idea 3: Proactive, Not Reactive, Detection

The Difference

50,000 threats
missed by legacy email security



792
internal email threats



16,140
credential theft attempts

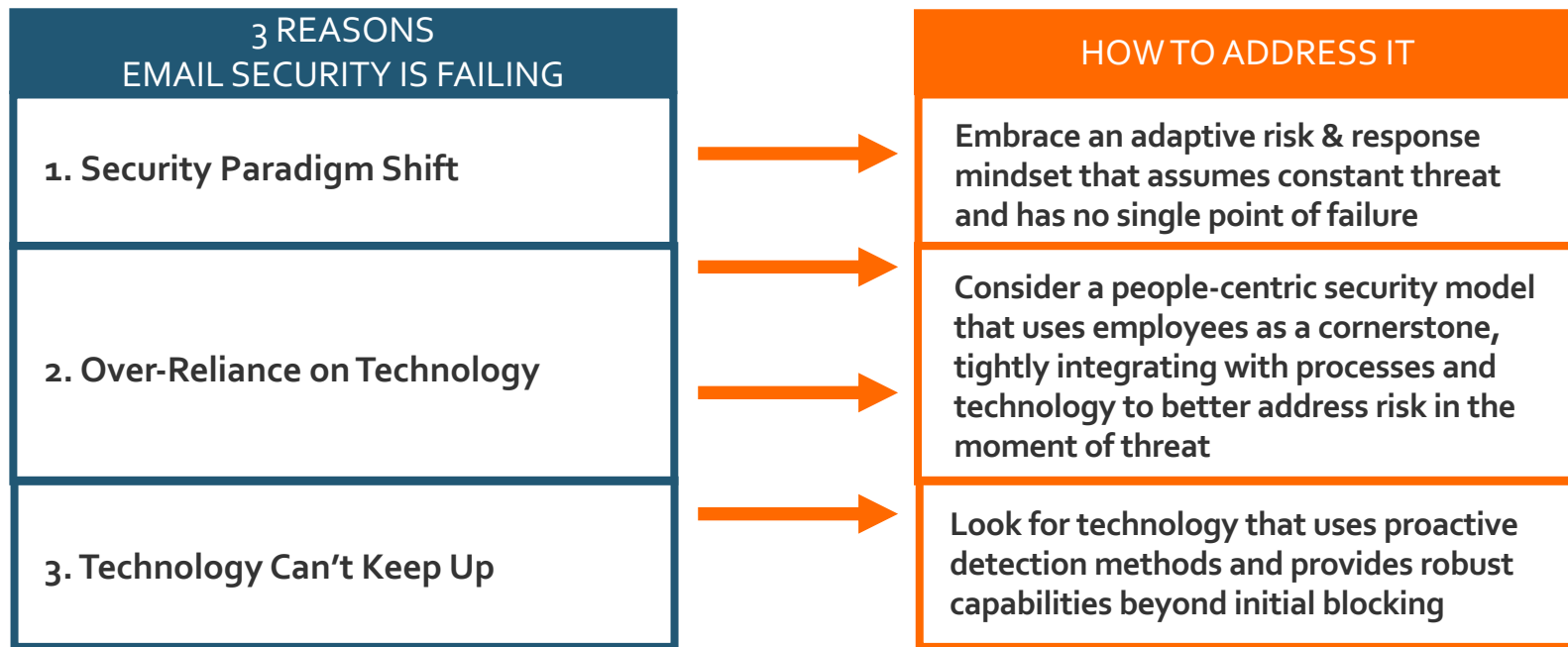


2,173
malicious URLs



21,281
business email compromise
attacks

Comprehensive Approach Addresses Critical Gaps



Multiple layers of defense returns trust back to the inbox and time back to the security team

About GreatHorn

GreatHorn Email Security is a threat detection and response platform for protecting organizations *Before, During,* and *After* an email attack.

CONTACT INFO:

greathorn.com
info@greathorn.com
855-478-4676

