Mighty Guides

Sponsored by

IRONSCALES
SAFER TOGETHER

How to Stay Ahead of the Growing E-Mail Security Threat

Table of Contents

Introduction

Email is so necessary to our daily business lives that using it has become as routine as breathing. And just as breathing exposes you to all sorts of airborne disease, clicking a link in an email message can expose you or your organization to infection. It happens a lot, and the incidence of "cyber-infection" by email is increasing.

According to Federal Bureau of Investigation statistics, reports of successful phishing attacks more than doubled between 2019 and 2020.[1] The latest research from the Verizon 2021 Data Breach Investigations Report finds that "Eighty-five percent of breaches [in this year's report] involved the human element. Phishing was present in 36% of breaches in our dataset, up from 25% last year. Business Email Compromises (BECs) were the second-most common form of Social Engineering. This reflects the rise of Misrepresentation, which was 15 times higher than last year."[2] These trends continue even though companies spend more time and money on email security than ever before.

This eBook takes a closer look at why email continues to be the number one attack vector favored by cybercriminals. It also looks at why more layers of email security fail to prevent these sophisticated attacks, and it discusses a new approach to email security that is meeting with success.

If you have a stake in the security of your organization's email system, you'll find value in this brief but insightful discussion of the topic.

All the best,
David Rogelberg
Editor,
Mighty Guides Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Foreword

Phishing attacks remain the single biggest cybersecurity threat your company faces today. Every day criminals launch billions of new phishing attacks. No company is immune. Legacy solutions like Secure Email Gateways can't keep up. Even the most advanced email security capabilities available with O365 struggle to stop advanced attacks like Business Email Compromise, Account Takeover and VIP impersonation. IRONSCALES' powerfully simple email security solution was built to help keep your O365 email safe.

Verizon's 2021 Data Breach Investigations Report found that "Social attacks as a pattern have continued to increase since 2017, with Business Email Compromise (BEC) breaches doubling again since last year. Web-based email is a favorite target."

We commissioned this Mighty Guide so that you could hear from your peers in the field about the experiences they've had with securing their own web-based email, specifically O365. They detail their experiences to date, including where existing solutions have fallen short.

Enjoy the book!

Regards,
Eyal Benishiti,
CEO,
IRONSCALES

FREE 90 DAY SCAN BACK:

Discover dormant threats in your organization

Get your free scan today at
https://ironscales.com/demo/90days →

IRONSCALES
SAFER TOGETHER

Meet Our Experts

Eyal Benishti
CEO, IRONSCALES

Mark Eggleston
Vice President, Chief Information Security and Privacy Officer, Health Partners Plans

Vito Sardanopoli
Managing Principal and Founder, Vantage CyberRisk Partners, LLC

Chuck Brooks
President, Brooks Consulting International

Jeff Farinich
SVP Technology Services and CISO, New American Funding

Joe Minieri
Chief Information Security Officer, Orvis

Scott Morgan
Information Security Officer, Florida Department of Highway Safety and Motor Vehicles

Chapter One

Email Is a Cybercriminal's Best Friend

It's true: Cybercriminals love email, and it's easy to see why. Phishing and other kinds of socially engineered email attacks make cybercrime a lot like stealing candy from babies. Here's why:

- 97 percent of email users cannot recognize a sophisticated phishing email.[3]
- Only 3 percent of email users ever report phishing emails to their managers.[4]
- Phishing works: Almost a third of all phishing emails are opened.[5]

This is why email has become the number one attack vector for cybercriminals, accounting for 95 percent of all cyberattacks directed against enterprises.[6] These attacks are so successful that email attack strategies are evolving to make them even harder to detect. Just a few years ago, the most common way to deliver malware in an attack email was through a malicious attachment, but improved network intrusion prevention tools are often able to detect and block these attachments. The attachment strategy has largely been replaced by email messages with links to malicious websites.

How do you know if you've been attacked? It's not always so easy to tell. Here's an example.

You receive an email from someone in your company whom you recognize asking you to download and review a document before your next meeting. The email includes a link to the website of a company you also recognize, where you are asked to fill in your email address. You go to the landing page for a downloadable whitepaper, type your email, and select Download.

"Criminals prefer email attacks because email is such a widespread form of communication. With literally billions of email addresses globally, the target is wide and the chance of success is high, depending on the sophistication of the phishing attack."

Scott Morgan,
Information Security Officer,
Florida Department of Highway Safety and Motor Vehicles

A message pops up saying that the document will be emailed to you soon. You check your inbox, but the document is not yet there. You return to your work and forget that you are expecting this document, which never arrives.

Six months later, you learn that your company has experienced a breach that appears to have been underway for months. Security teams are still trying to learn what has been compromised. The attack apparently began as a sophisticated spear phishing campaign. By the time you learn about the attack, you may have no recollection of the time you selected a link in an email several months ago.

> **People are being trained to recognize phishing emails. The problem is that the phishing attacks we see today, those emails are just too good.**
>
> 
> **Eyal Benishiti,**
> CEO, IRONSCALES

Email attacks are so pervasive that security analysts now spend a significant percentage of their work time investigating email-related alerts. To stay on top of these threats, companies add more email security tools, such as secure email gateways (SEGs) and Microsoft Defender for Office 365 (formerly Microsoft Advanced Threat Protection), and more security analysts. Yet, the number of successful email attacks continues to grow.

So, what's the answer? To protect yourself against these sophisticated attacks, it's important to understand why they are so effective and why traditional tools fail to stop them.

"Attacking through email is easy to do and it works. It is a percentage game for malicious hackers. Out of thousands of emailing phishing attacks, it only takes one victim to enable a breach. Also, cybercriminals now have the machine learning tools to automate email cyberattacks, making their odds of breaking through much higher."

Chuck Brooks,
President, Brooks Consulting International

> We are long past the era of fake princes in a faraway land saying that you are the beneficiary in a will or winner of a lottery. Phishes nowadays are usually quite difficult to recognize as fake because the emails are tailored to your personal background and interests. They are easy to click because they are relatable.

Chuck Brooks,
President, Brooks Consulting International

Key Points

- Cybercriminals love email because it provides easy access to targets, most people do not recognize phishing emails, a third of the people who receive phishing emails open them, and few people report malicious emails to their managers.
- Email attacks are so pervasive that security analysts now spend a significant percentage of their work time investigating email-related alerts.
- Even though companies add more email security tools such as secure email gateways (SEGs) and Microsoft Defender for Office 365 (formerly Microsoft Advanced Threat Protection), the number of successful email attacks continues to grow.

"The right ICES (Integrated Cloud Email Security solution) can pay dividends in the identify-detect-block-train activity provided by the integrated solution."

Scott Morgan,
Information Security Officer, Florida Department of Highway Safety and Motor Vehicles

Chapter Two

Inside the Email Security Challenge

Securing email is inherently difficult for two reasons:

- Email is designed for convenience, not security. Email communications use an open data format so that users can send and receive messages to anyone, anywhere, regardless of the devices or email programs they use. When you receive an email message, every server and service provider that touches that message on its way to you has complete access to the message contents and basic email properties, such as the From field in the email header. It's important to understand that the From field is not necessarily related to who actually sent a message. There is nothing preventing anyone from sending an email with someone else's name in the From field.

> **More and more organizations use cloud services as their go-to email solution, and being in the cloud, such solutions are really exposed. More scripts and automation have enabled cybercriminals to become sophisticated about how they monetize a successful attack.**

Eyal Benishiti,
CEO, IRONSCALES

"The best phishing messages are crafted manually and usually with intimate knowledge of the intended target. The more you know, the further you can go: It is the result of highly targeted and intimate attacks."

Scott Morgan,
Information Security Officer,
Florida Department of Highway Safety and Motor Vehicles

- Email users trust their email. After spending roughly half of their work time, day after day, sending and receiving emails, people come to believe that the messages they receive are what they appear to be. Most of the time, they are. It is this trust in email that makes people vulnerable to the socially engineered email attack. Then, when a colleague sends a message asking us to download and review a document before the next meeting, we don't think twice about it.

> **Attacks through email are becoming more sophisticated—and more common. It's still the number one vehicle for cybercriminals to get inside an organization.**
>
> 
>
> **Eyal Benishiti,**
> CEO, IRONSCALES

On the technology side, tools are readily available that filter spam, block attachments that contain known threats, and detect unusual patterns that may indicate that an attack is underway. You can also implement email encryption to protect message contents.

The biggest threat, however, is the one most difficult to block: the socially engineered attack that plays on people's trust of their email. These attacks are designed to fool us into giving up passwords, credentials, proprietary information, or money or to select something that launches a malicious payload—and the deceptions are getting better.

As major email applications become cloud based, email accessibility becomes easier for users. It also becomes easier for attackers to identify and target users with socially engineered attacks. The following table shows the most common types of attack.

"When doing cost comparisons, consider the number of users, the advanced email controls you want, and other areas that overlap email security such as data loss prevention, cloud storage, retention and archival costs."

Mark Eggleston,
Vice President, Chief Information Security and Privacy Officer, Health Partners Plans

Attack Type	Description
Phishing	An email that looks like it came from a legitimate source, designed to fool someone into giving up personal information. Variations include: • **Spear phishing.** A phishing email targeted at a particular person or employee. • **Whaling.** Phishing emails, often personalized, that target high value employees.
Spoofing, Impersonation, and Account Takeover	Disguising an email to appear as if it is from a known source. These strategies are widely used in phishing attacks. Varieties include: • **Email spoofing.** The attacker changes the header to display a sender email address with a genuine domain name. Many attacks also use website spoofing. • **Email impersonation.** The attacker changes the header to display a sender email address with a domain name that looks almost like the real thing. Phishing attacks can also use brand impersonation. • **Account takeover.** The attacker gains access to a legitimate account by using stolen credentials and sends phishing emails from that account.
Polymorphic attacks	Phishing attacks that use a burst of emails that automatically and randomly change properties, such as subject lines, sender names, and links in the email message. These attacks are specifically designed to defeat signature-based email security solutions, and they make up almost half of today's phishing attacks.
Business Email Compromise (BEC)	A targeted attack that uses spoofing and impersonation strategies for the purpose of committing financial fraud. The email usually includes instructions to send money. They can be difficult to detect because they often seem legitimate, such as a request for payment and an invoice from a known vendor.

Today's email security challenge is rooted in both technological and human weaknesses. An effective email security solution must address both.

"It is important to identify and factor in the specific policy configuration management resources needed to ensure effective deployment and ongoing governance of the email security solution."

Vito Sardanopoli,
Managing Principal and Founder,
Vantage CyberRisk Partners, LLC

> Choosing a good email security solution is very important because threats to the organization and the impact on users have to be minimized.

Jeff Farinich,
SVP Technology Services and CISO,
New American Funding

Key Points

- It's important to understand that the From field is not necessarily related to who actually sent a message. There is nothing preventing anyone from sending an email with someone else's name in the From field.
- Socially engineered attacks play on people's trust of their email. These attacks fool us into giving up passwords, credentials, proprietary information, money, or to select something that launches a malicious payload—and the deceptions are getting better.
- As major email applications become cloud based, email accessibility becomes easier for users. It also becomes easier for attackers to identify and target users with socially engineered attacks.

"Incorporating AI capabilities would increase the accuracy of threat detection because rule-based detection is always playing catchup with ever-changing evasive techniques."

Jeff Farinich,
SVP Technology Services and
CISO, New American Funding

Chapter Three

Why Most Email Security Solutions Fall Short

Most organizations address email risk by adding layers of technology, such as a SEG or Defender for Office 365. These solutions share a common weakness, however: They depend on policy configuration and static signature databases to identify threats. That means that they require a lot of policy management and upkeep to stay current with the latest threats. The speed at which attackers change their attack strategies makes keeping up impossible.

Defender for Office 365 is a good example. It requires extensive policy configurations to protect against any of the many varieties of phishing attacks. It enables you to designate email addresses for protection against impersonation, but each phishing policy requires its own list of protected addresses, and you cannot protect more than a combined total of 60 different email addresses across all your phishing policies. Defender for Office 365 offers no protection against polymorphic attacks, which now account for nearly half of all phishing attacks.[7]

The result is a costly, maintenance-intensive tool that will never be able to keep up with socially engineered attacks. Test data bears this out. In a test involving 1,000 phishing emails with malicious attachments or links, the time between when an attack was first reported and when Defender for Office 365 deployed a signature ranged from six days to more than eight months.[8] As Aberdeen research shows, 9.99 percent of clicks on phishing URLs happen within the first twenty-four hours of a phishing attack. That makes Defender for Office 365 an inadequate defense against phishing.

"No signature or rule- based security solution can keep up with the ever-changing attack techniques."

Jeff Farinich,
SVP Technology Services and CISO, New American Funding

Keep in mind that all these additional security tools generate a lot of alerts that security analysts must investigate. Between maintaining the tools and chasing down security alerts, analysts are spending most of their time focusing on email-related security issues.
To avoid alert fatigue, security teams often de-tune the tools so that they trigger fewer alerts. That cuts down on alerts, but it can also mask attacks.

Most email security solutions fail to protect against socially engineered attacks because they focus on the wrong things. Their reliance on policy configurations and monitoring of large-scale data patterns limits them to finding known security threats. For all the time it takes to configure and maintain them, these tools offer little protection against well-engineered, targeted phishing and BEC attacks.

To protect against those kinds of attacks, you need something entirely different.

"Historically, Office 365 Advanced Threat Protection lacked feature and accuracy parity with third-party email security vendors."

Jeff Farinich,
SVP Technology Services and CISO, New American Funding

“When we started using Office 365 for email, I didn’t trust Microsoft’s ability to provide sufficient email security. Email is a rapidly evolving threat. I believe it’s important to have that be the focus of the solution provider. Microsoft’s expertise is in delivering outstanding office and productivity products. Security is an add-on to its portfolio. I prefer a vendor whose primary mission is email security.”

Joe Minieri,
Chief Information Security Officer, Orvis

Key Points

- Most email security solutions depend on policy configuration and static signature databases to identify threats. They require a lot of policy management and upkeep to stay current with the latest threats. The speed at which attackers change their attack strategies makes keeping up impossible.
- Defender for Office 365 offers no protection against polymorphic attacks, which now account for nearly half of all phishing attacks.
- Most email security solutions fail to protect against socially engineered attacks because they focus on the wrong things. For all the time it takes to configure and maintain them, these tools offer little protection against well-engineered, targeted phishing and BEC attacks.

"A sophisticated attacker can spoof a signature-based email security system. A policy of holistic cyber hygiene is required to help defend your email."

Chuck Brooks,
President, Brooks Consulting International

Chapter Four

How an Integrated Cloud Email Security solution Stays Ahead of Evolving Threats: Focus on the Inbox

There is one place where both technical and human elements of the email security challenge come together: the individual email user's inbox.

An integrated cloud email security solution (ICES) combines technical and human detection and response into a single platform that investigates email traffic at the inbox level. Here's how it works:

- Technical detection and response. Every email user has a unique pattern of inbound email. To identify an attack that has never been seen before and has no known signature, you must monitor and analyze email traffic across the entire organization, right down to each individual user's inbox. The ICES does this automatically in real-time, using artificial intelligence (AI)–powered detection and response technology. The key to capturing a high percentage of attacks is using AI algorithms optimized for the task, essentially being inside the inboxes of every email user. In our case, IRONSCALES can catch 99 percent of socially engineered email attacks in this way.

"The accuracy of blocking is critical because false-positives can have a significant impact on revenue generation in high-volume sales environments."

Jeff Farinich,
SVP Technology Services and CISO, New American Funding

- Human detection and response. For maximum effectiveness, you also need a machine-human feedback loop that includes both security analysts and email users. This feedback loop enables users to flag suspicious emails they receive and analysts to assess the flagged messages in real-time. Users receive real-time notifications on items they flag and any valid attack emails that land in their inbox. The platform itself becomes a continuous training tool for users, keeping them aware of and alert to the possibility that they may be the target of a phishing attack. The feedback loop also continuously refines the AI detection and response algorithms. By integrating human and technology elements in this way, IRONSCALES brings the catch rate close to 100 percent.

The best ICESs can be implemented in minutes and require no configuration. IRONSCALES ingests and analyzes ninety days of email history to establish a baseline for each user's mailbox. Within minutes, our AI algorithms gain deep awareness of email usage patterns at the inbox level in any email environment.

> **Most email security solutions try to detect an indication of compromise. This is intelligence-based threat detection. But, if an attacker is using social engineering to make someone do something they are not supposed to do, the only way you are going to know that and block it is if you are inside that email user's mailbox.**

Eyal Benishiti,
CEO, IRONSCALES

"Consolidating email security tools into one solution from a single provider often results in the most cost- effective approach to acquiring an email security solution. The solution needs to be effective, and you need to weigh the risk of your single provider becoming a single point of failure."

Vito Sardanopoli,
Managing Principal and Founder,
Vantage CyberRisk Partners, LLC

Good ICESs perform basic email security functions, such as spam detection, malware and virus detection, attachment inspection, and sandboxing. They also support autoremediation. Their real strength, however, is in detecting sophisticated attacks that include spoofing and impersonation, polymorphic attacks, and suspicious email clustering. Good ICESs also include phishing emulation, simulation, and training, and they integrate with all widely used email platforms in cloud, on-premises, and hybrid environments.

> **We apply machine learning at the mailbox level to learn unique patterns of each individual email user. We detect unusual emails this way. We use the platform to create a community of security teams that work collaboratively but anonymously to identify difficult-to-detect trends.**

Eyal Benishiti,
CEO, IRONSCALES

This all sounds great, but do you really need another email security tool?

To gain maximum protection against sophisticated socially engineered phishing and BEC email attacks, you need a top-performing ICES. Policy-based tools such as Defender for Office 365 offer little protection against these kinds of attacks, but there's an additional advantage to the ICES approach. The right solution can help you simplify your security stack by consolidating tools, reducing overall technology costs and the time spent configuring and maintaining all those tools.

"By combining AI and human intelligence, you get a more comprehensive and effective approach to filtering phishing attacks and can ultimately help your organization defend against and respond to such email-based attacks."

Vito Sardanopoli,
Managing Principal and Founder,
Vantage CyberRisk Partners, LLC

> Real-time feedback from integrated online security awareness services can train users in real-time so that they can avoid real attacks. Security departments need to make such training fun and engaging, but they must deliver training that is meaningful to users so that they avoid disaster.

Scott Morgan,
Information Security Officer, Florida Department of Highway Safety and Motor Vehicles

Key Points

- To identify an attack that has never been seen before and has no known signature, you must monitor and analyze email traffic across the entire organization, right down to each individual user's inbox.
- For maximum effectiveness, the ICES needs to provide a machine-human feedback loop that includes both security analysts and email users. Users receive real-time notifications on items they flag and any valid attack emails that land in their inbox. The platform itself becomes a continuous training tool for users.
- The best ICESs can be implemented in minutes and require no configuration. IRONSCALES ingests and analyzes ninety days of email history to establish a baseline for each user's mailbox within minutes.

"A deployment that is highly complex or not well defined can have a considerable negative impact on the overall deployment initiative, imposing additional, unnecessary costs and delays."

Vito Sardanopoli,
Managing Principal and Founder,
Vantage CyberRisk Partners, LLC

Chapter Five

How an ICES Like IRONSCALES Keeps You More Secure at Lower Cost

A good ICES saves time and money in ways that can benefit both business adopters and security service providers.

For businesses, an ICES significantly lowers the risk of being victimized by a sophisticated phishing attack that may be ransomware; part of a more subtle attack designed first to infiltrate, and then to exfiltrate sensitive data; or a targeted BEC attack designed to take your money.

In addition to risk reduction, the IRONSCALES ICES is easy to implement, requires no configuration or policy maintenance, catches a high percentage of attacks automatically through AI algorithms, and remediates a significant percentage of email anomalies. These all contribute to a significant savings in labor required to manage email security. We have found that IRONSCALES can reduce time spent in manual email analysis by 90 percent.

> **Instead of augmenting an email security gateway, you can get rid of it altogether.**
>
> 
>
> **Eyal Benishiti,**
> CEO, IRONSCALES

"Tuning is a time- consuming process. Costs to consider are impact to users when threats get through, email false-positive blocks, hours that email administrators waste, and additional consulting statements-of-work with support vendors."

Jeff Farinich,
SVP Technology Services and CISO, New American Funding

For service providers, an ICES is a low-cost technology that managed services providers (MSPs) and managed security services providers (MSSPs) can add to their portfolio of security offerings. It provides a highly effective managed email security solution that quickly adapts to the unique usage patterns and threat environments of their clients.

To learn more about how an ICES can simplify your security stack, reduce the burden of email security monitoring and remediation, lower costs, and greatly improve your security posture please visit www.ironscales.com.

"If you are migrating to E5 solely for robust email security, it would likely cost you more than a stand-alone secure email gateway."

Mark Eggleston,
Vice President, Chief Information Security and Privacy Officer, Health Partners Plans

> The best way to control email security costs is to reduce the people cost through quality AI and a detailed auditing/tracking system. Keeping my security team and my company productive is paramount. When the email security system isn't performing this task optimally, my security team must manually redisposition suspect email or, worse, conduct incident response and recovery.

Joe Minieri,
Chief Information Security Officer, Orvis

Key Points

- To provide companies with the security and value they need, an ICES must easy to implement, require no configuration or policy maintenance, and catch/automatically remediates a high percentage of attacks through AI algorithms.
- An ICES significantly lowers the risk of being victimized by a sophisticated phishing attack that may be ransomware, part of a more subtle attack designed first to infiltrate and then exfiltrate sensitive data, or a targeted BEC attack designed to take your money.
- IRONSCALES is a low-cost technology that Managed Services Providers (MSPs) and Managed Security Services (MSSPs) can easily add to their portfolio of security offerings. It is a highly effective managed email security solution that quickly adapts to the unique usage patterns and threat environments of their clients.

"Tools can be preventive, and consolidation combined with orchestration can enable quick response to incidents. Having everything accessible in one place simplifies the cybersecurity process and makes analysts' jobs much easier. People are still the biggest cost, which is why automation is a good way to mitigate risks and expenses. The biggest cost, though, is being breached, with all the implications for reputation and the bottom line."

Chuck Brooks,
President, Brooks Consulting International

Learn More About Our Experts

Eyal Benishti, CEO at IRONSCALES

As chief executive officer of IRONSCALES, Eyal Benishti pioneered the development of the world's first self-learning antiphishing email security solution for automatic prevention, detection, and autonomous incident response to cyberattacks. Before founding IRONSCALES in 2013, Eyal was a security researcher and malware analyst and held many R&D roles. He holds a bachelor's degree in computer science and mathematics from Bar-Ilan University in Israel.

Mark Eggleston, Vice President, Chief Information Security and Privacy Officer, Health Partners Plans

Mark Eggleston is a senior executive specializing in security and privacy program management. Vice president and chief information security officer at a Philadelphia HMO, he leads the implementation of security technologies and privacy initiatives, manages business continuity, and oversees disaster recovery and facility management. Mark holds anMSW and a postbaccalaureate certificate in management information systems from Virginia Commonwealth University.

Vito Sardanopoli, Managing Principal and Founder at Vantage CyberRisk Partners, LLC

Vito Sardanopoli is an accomplished executive with broad expertise in cybersecurity, IT, information management, and enterprise risk management. He has helped build cybersecurity capabilities for health care, financial services, and retail organizations, even serving as an appointed member of the US Department of Health and Human Services Health Care Industry Cybersecurity Task Force. Vito holds an MBA from New York University Stern School of Business.

Chuck Brooks, President, Brooks Consulting International

Chuck Brooks is a globally recognized thought leader and subject matter expert cybersecurity and emerging technologies. He was named a Top 50 Global Influencer in Risk, Compliance by Thompson Reuters and the #2 Global Cybersecurity Influencer by IFSEC. Chuck is a cybersecurity expert for "The Network" at the Washington Post, visiting editor at Homeland Security Today, and a contributor to FORBES.

Jeff Farinich, SVP Technology Services and CISO at New American Funding

Jeff Farinich is a seasoned Information Technology & Security leader with over 25 years of experience spanning the high-tech, financial services, employment & recruiting, and entertainment industries. He joined New American Funding in 2019 overseeing corporate IT and cybersecurity. Jeff earned a MBA from University of Southern California and holds PMP, CISSP, CISM and CISA certifications.

Joe Minieri, Chief Information Security Officer at Orvis

Joe Minieri is the Orvis Company's Chief Information Security Officer. In this role Minieri leads Orvis's Information Security & Compliance team responsible for the retailer's cyber security and privacy program. Minieri has also held information security leadership roles at L.L. Bean and General Dynamics, as well as being part of several ecommerce & technology start-ups. He is a graduate of Georgia Institute of Technology and Boston University.

Scott Morgan, Information Security Officer at Florida Department of Highway Safety and Motor Vehicles

Scott is currently the Information Security Officer for a government agency, as well as a former CIO. Scott has over 20 years of experience in information security operations, governance, and leading organizational change in various organizations. Scott holds numerous information security certifications, as well as a B.S. and M.A in Public Administration Leadership.


Partner with IRONSCALES
Phishing attacks are the biggest threat your customers face today. IRONSCALES offers a powerfully simple anti-phishing solution that is fast to deploy, easy to use and protects your customers against today's most dangerous phishing threats.
Partner Benefits
Short sales cycles
Bulk pricing
Easy access to POCS and demos
Ongoing training & support
Multi-tenant MSSP deployments
"IRONSCALES' comprehensive artificial-intelligence phishing protection is aligned with our Dark Rhino promise on delivering value through innovation, so this partnership is a big win for us and our customers.
Kevin Casey,
CEO of Dark Rhino Security
Learn more at https://ironscales.com/partner-program/