SECURITY

PHISHING DEFENSE AND GOVERNANCE

How to Improve User Awareness, Enhance Controls and Build Process Maturity

TERRANOVA SECURITY

ISACA®

CONTENTS

4 **Introduction**

4 / Key Findings

5 **Current Anti-phishing Landscape**

7 **Optimization of Defenses**

7 / Blending Internal and External Expertise

8 / Better Defense Through Better Management

9 / Implementing Improvements to Phishing Defense

10 **Conclusion**

11 **Acknowledgments**

© 2019 ISACA. All Rights Reserved.

ABSTRACT

Phishing attacks are increasing rapidly in severity and prevalence. To determine how enterprises are defending against phishing attacks, ISACA® surveyed a global population of security, assurance, risk and governance professionals in November 2018. This white paper provides you with information about the survey results—strategies that enterprises employ for phishing defense, how they manage those strategies and key implications that impact their decisions about both. For example, one key potential impact that the survey results show is that the majority of respondents are less than fully confident in their enterprises' overall phishing awareness programs. The survey findings also reveal a potential disconnect between the development of phishing awareness training material and the management of phishing awareness efforts. This white paper also gives you recommendations on potential improvements to phishing defense, such as increasing management, and overall maturity, of defense techniques.

© 2019 ISACA. All Rights Reserved.

Introduction

Phishing and email-borne attacks, already a huge problem for many enterprises, are increasing. For those unfamiliar with phishing, it consists of using email as a vehicle for attack—including, for example, fraudulent attempts to obtain sensitive information (e.g., credit card details), as a vehicle to deliver malware, or as an instrument to trick users into divulging their credentials. These attempts may be disguised as originating from a trustworthy sender in an attempt to make success more likely.

The US Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) revealed in July 2018 that global losses from financial phishing attacks topped 12-billion dollars, with a rate of expansion of 136 percent between December 2016 and May 2018.[1]The FBI data pertain to only a subset of phishing attacks: specifically, Business Email Compromise (BEC) and E-mail Account Compromise (EAC)—both attacks that attempt financial fraud using phishing as their primary vehicle. The phishing problem in aggregate—including all types of phishing attacks and not just these two subsets —is much more substantial. For example, the Verizon *2018 Data Breach Investigations Report* reveals that 92.4 percent of malware is delivered via email.[2] Also, the Symantec™ *2018 Internet Security Threat Report* (ISTR) shows that, at the close of 2017, the average email user received 16 malicious emails per month.[3]

The reason why cyberattackers use phishing attacks so predominantly is these techniques work, which the FBI IC3 data corroborate. The ongoing effectiveness of these attacks (i.e., why email users continue to be susceptible to phishing attacks) is more complicated to determine—particularly considering the large amount of effort and funding that many enterprises have invested (and continue to invest)—in phishing mitigation.

Key Findings

ISACA survey responses indicate trends that help explain why email users continue to be susceptible to phishing attacks:

- **Key components are often missing**—Awareness efforts and training are prevalent, but simulation is not used often. The most common methods employed to prevent phishing are employee training (71 percent), online learning solutions (64 percent), and email newsletters (63 percent). Only 57 percent of the survey-respondent enterprises perform phishing simulation, and only 25 percent employ active knowledge-based assessment of employee phishing knowledge.
- **Different resources are employed in awareness material development and awareness program execution**—Enterprises typically outsource development of phishing awareness materials, but use internal staff to manage the program. Only 38 percent of respondents indicate that their enterprises develop security awareness activities completely internally (i.e., using internal resources to develop security awareness and anti-phishing materials), but 85 percent said that the execution and management of their enterprise security awareness program is internal. This can lead to challenges with ensuring that the security awareness program is managed optimally. This is because the resources (and management and governance structures) that are used to develop awareness program content and tools are different from the resources that use that content and tools to execute the awareness program.

This white paper examines these and other trends with the objective to extrapolate potential improvements to phishing defenses, and optimize anti-phishing management and governance practices.

[1] Department of Justice, Federal Bureau of Investigation; "Public Service Announcement: Business E-mail Compromise the 12 BIllion Dollar Scam," Alert Number I-071218-PSA, 12 July 2018, www.ic3.gov/media/2018/180712.aspx

[2] Verizon, *2018 Data Breach Investigations Report*, 11th edition, 2018, https://enterprise.verizon.com/resources/reports/dbir

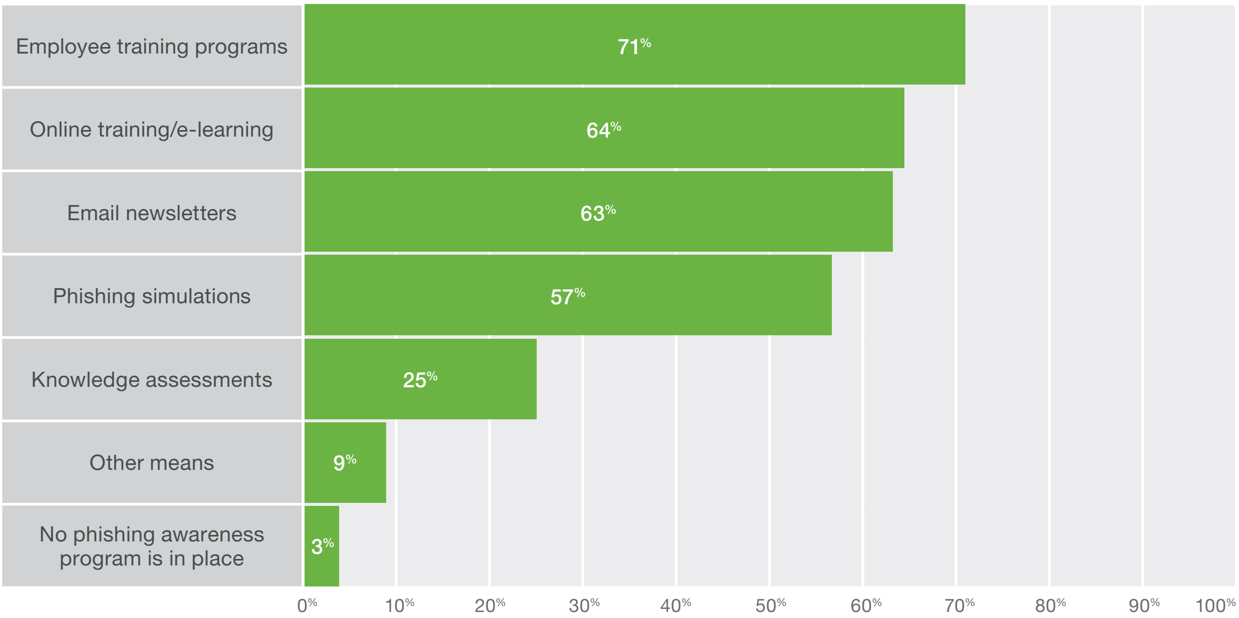
[3] Symantec, *Internet Security Threat Report*, volume 23, March 2018, www.symantec.com/security-center/threat-report

© 2019 ISACA. All Rights Reserved.

Current Anti-phishing Landscape

In a recent ISACA survey, respondents report that the anti-phishing controls that they deploy most frequently target employee awareness. Seventy-one percent of respondent enterprises use employee training, 64 percent use online learning solutions and 63 percent use email newsletters to promote phishing awareness and mitigate phishing threats as part of their anti-phishing strategy (**figure 1**). (Note that respondents were instructed to select all applicable answer choices.)

FIGURE 1: Methods Used to Promote Phishing Awareness and Mitigate Phishing Threats



Seventy-five percent of enterprises measure and regularly report on the effectiveness of their phishing awareness programs. The level of confidence in the effectiveness of the programs being measured and reported on, however, was low. Only 45 percent of respondents are either completely confident or very confident in their abilities to accurately assess the effectiveness of phishing awareness efforts with only 12 percent of those surveyed being completely confident (**figure 2**).

The development of the anti-phishing program content and tools is either completely outsourced (developed by a partner or service provider) or a combination of the enterprise with external resources. Only 38 percent of respondent enterprises develop their security awareness materials completely internally (i.e., using internal resources to develop security awareness and anti-phishing materials (**figure 3**).

Once the materials are developed, management of the security awareness program is considered. The majority of respondents manage their security awareness programs internally, using materials that were developed by, or with, others who are external to their enterprise. However, slightly over a quarter (28 percent) of respondent enterprises are in the process of moving security awareness program management for these controls to an outside vendor or are considering this move (**figure 4**).

© 2019 ISACA. All Rights Reserved.

Overall, the development of materials and the collaboration on program management is a model that is, in some ways, analogous to the use of cloud providers in a technology context, i.e., the enterprise uses internal management resources and principles to operate, and internal governance structures to oversee, elements of their operational security that are developed by external resources. Similar to cloud deployments, anti-phishing strategies and awareness programs require shared responsibility to be optimally effective, and this is where the lack of confidence in assessing the effectiveness of phishing awareness programs and the relative weakness in ability to measure and report on their effectiveness affect the success of anti-phishing programs.

FIGURE 2: Accurately Assessing the Effectiveness of Phishing Awareness Programs

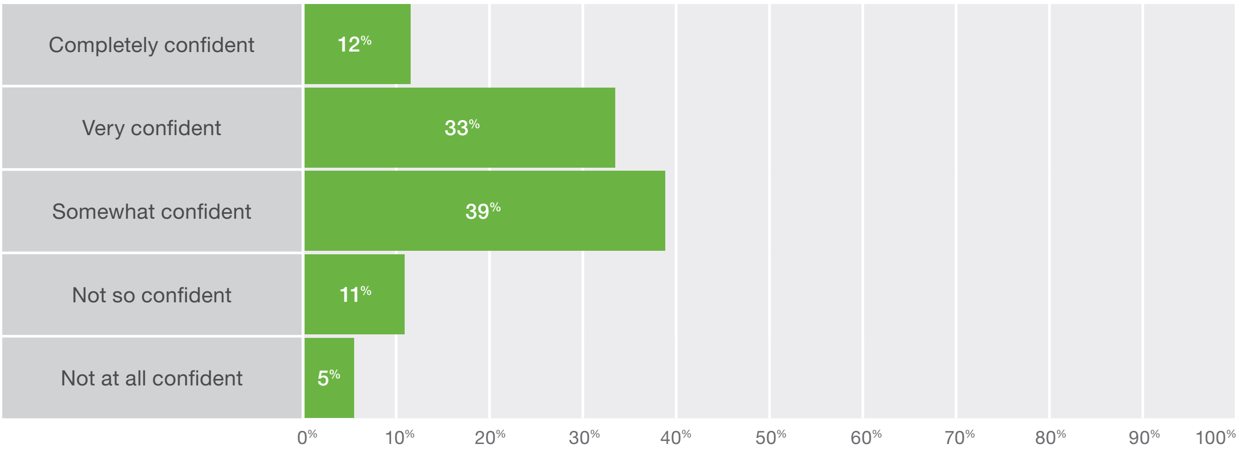


FIGURE 3: Development of Security Awareness Program Content and Tools

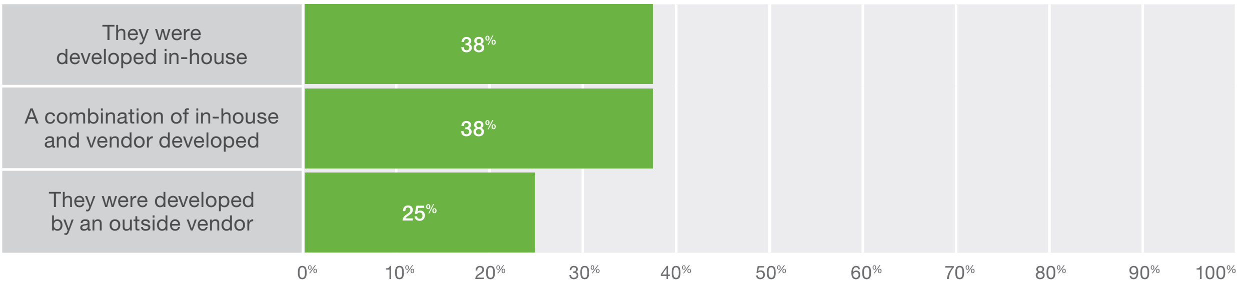
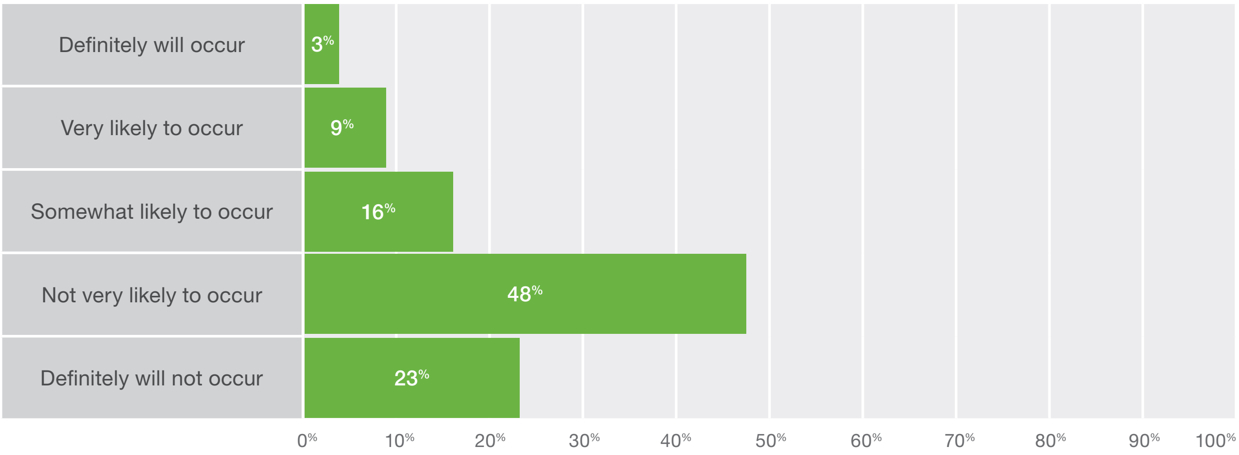


FIGURE 4: Movement of Security Awareness Program Management to Outside Vendor in Next 12 Months



© 2019 ISACA. All Rights Reserved.

Optimization of Defenses

The survey data reveals an interesting implication about phishing. The mechanisms that empirically validate the performance of awareness efforts (e.g., knowledge assessment and phishing simulation) are employed less frequently than controls to increase phishing awareness. So, increased focus on empirical validation may help security teams calibrate efforts over time. Although this implication is not directly provable via the survey data, a virtuous cycle of measurement and improvement over time is a long and well-established foundational principle of good governance and, therefore, can potentially add value by helping to establish this feedback loop.

If this implication is true, the question becomes, "what can a practitioner do to improve?" One strategy that shows promise is to selectively and strategically leverage service provider relationships where appropriate. This strategy is compelling because external service providers have advantages in specialization and economies of scale that are not available to internal teams. Unless an enterprise's core competency is phishing (which is not usually the case), changes in attacker tradecraft, attacker motivation, delivery vehicles, etc. will likely outpace an internal team's ability to research those changes. A reliable, well-staffed external team can focus on keeping pace with developments in attacker activity and their methods of operation. This is similar to external specialists who can more effectively focus on and leverage economies of scale (compared to internally-sourced efforts), when researching malware or zero-day vulnerabilities.

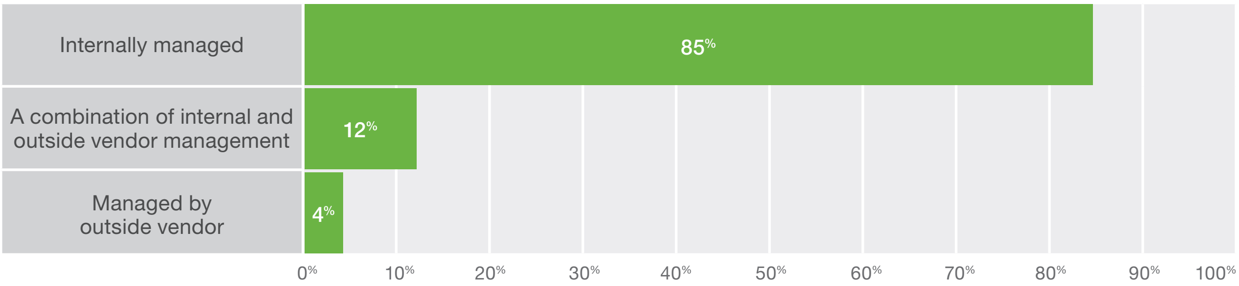
One strategy that shows promise is to selectively and strategically leverage service provider relationships where appropriate.

Blending Internal and External Expertise

Strategically leveraging service provider relationships does not imply that there is not a role for enterprises in anti-phishing strategies. To the contrary, internal staff know the enterprise's business and employees better than any external service provider ever will. As a result, internal staff are best equipped to understand the needs of their users, any enterprise-specific training requirements and the methods that are most effective to reach each user population. Given that external service providers can specialize in ways that are challenging for internal teams, and internal teams have a better insight into the enterprise and the needs of its employees, blended strategies that leverage both sets of strengths can have advantages.

The ISACA survey data show significant reliance on service providers for the development of program content and tools (see **figure 3**), however, enterprises are more likely to manage their security awareness programs internally. Specifically, only four percent of survey-respondent enterprises outsource all management of awareness activities and 12 percent use a combined approach, involving internal and external resources (**figure 5**).

FIGURE 5: Security Awareness Program Management



© 2019 ISACA. All Rights Reserved.

Enterprises, however, can benefit from the expertise of service providers. Models of how enterprises may engage service providers include:

- **Use of external providers for validation only—**One or more service providers validate the effectiveness of user behavior modification. These services include phishing simulation (i.e., testing user behavior through the use of phishing-like emails to gauge user resilience to phishing) and knowledge-based assessment of the user.
- **Use of external providers for awareness material development—**One or more service providers develop security-awareness training materials, awareness collateral (e.g., posters, email notifications and screensavers) and other specific artifacts designed to support the program.
- **Use of external providers for management—**One or more service providers manage, track, measure and report on user engagement with security awareness materials (e.g., class or training attendance and tracking information emails to users) and manage validation campaigns over time.
- **Turnkey service provider approach (fully outsourced)**—Use of typically one service provider to fully manage the entire phishing defense (security awareness) program.

Each model has potential advantages and disadvantages. Likewise, each model requires solid execution and management support to employ optimally. To evaluate whether the use of service providers is generating the value expected, the ability to test and manage their work is paramount, including the individual anti-phishing elements in the program (e.g., individual training or awareness material) and the overall management and governance of the program.

Better Defense Through Better Management

Building better phishing defenses and implementing better management of those defenses vary from enterprise to enterprise, depending on numerous factors, many of which are enterprise-specific. For example, enterprises have different risk appetites, cultures and types of employees, and operate in different industries. Despite these differences, better management, measurement and validation have an almost-universal positive impact on phishing defense. This positive impact comes with maturity, for two reasons:

- More mature processes are more likely to have mechanisms already in place that allow the performance of those processes to be measured and improved.
- Where the enterprise falls on the maturity spectrum impacts where and how improvements are best made. Bigger return on investment is likely realized by targeting specific areas that are lower on the maturity spectrum—improvements to an area that is relatively immature can be realized for less time, effort and expense relative to higher maturity areas. The overall maturity of the phishing defense program comprises various processes—some of which an enterprise may manage and some of which may be managed by service providers. Areas where an enterprise may be mature, but a supporting service provider is immature (or vice versa) represents an area where the enterprise can improve the overall maturity of the program by selectively refining the immature elements.

Enterprises tend to vary on the maturity spectrum over time. Enhancements in focus, investment or staff support tend to increase maturity, whereas decreasing those same resources likely reduces maturity. It is tempting to view this as a progression, where an enterprise moves from less mature to more mature over time. However, this is not always the case. Forces outside of the direct control of the enterprise can reduce maturity (e.g., loss of key staff and reduced budget), and a shift from one service provider to another can cause maturity to increase or decrease, depending on the capabilities of the providers selected.

To determine where the individual elements within a program fall on the maturity spectrum, the enterprise can systematically analyze the program elements in the same way it analyzes other sets of security controls or any other processes in the enterprise. Any methodology that allows for systematic examination of maturity can be used (e.g., COBIT®[4] or CMMI®[5]), but it is particularly important to factor in various co-sourced or outsourced relationships

[4] ISACA, "Introducing COBIT® 2019," http://www.isaca.org/cobit/pages/default.aspx
[5] CMMI, "CMMI® Institute," https://cmmiinstitute.com/

© 2019 ISACA. All Rights Reserved.

as part of this evaluation. If service providers are used, the reporting and instrumentation provided by them must be clearly understood. To the extent that service providers improve maturity, the enterprise must make full use of any technical integration that the service providers may provide, such as customization features to yield better engagement from users and integration with automated workflows.

To determine where the individual elements within a program fall on the maturity spectrum, the enterprise can systematically analyze the program elements in the same way it analyzes other sets of security controls or any other processes in the enterprise.

Implementing Improvements to Phishing Defense

The ISACA survey data suggest several methods to improve the management and governance of phishing defense strategies. (Note that these methods are not the only steps that can be taken for improvement; however, they are steps that may provide benefits for a number of enterprises.)

- **Build in validation of phishing awareness campaigns.** If an enterprise is not already validating performance (e.g., through phishing simulation), it can bolster performance by ensuring that it has that capability. If an enterprise does have these measures in place (whether developed internally or by a service provider), the enterprise should ensure that it is able to correlate data about that performance to information about user engagement. This correlation allows the enterprise to gauge performance of awareness materials relative to each other. For example, suppose an enterprise knows users are reading awareness-oriented email bulletins about spear phishing, but validation efforts suggest that users continue to click on simulated spear phishing emails. In this case, awareness emails may not be having the desired effect. This provides the enterprise with important information upon which they can act, for instance, by offering just-in-time training. As enterprises track this information, phishing awareness activities are optimized over time and the enterprise can determine the most effective strategies for its user population.
- **Evaluate the existing outsourcing or co-sourcing relationships.** Determine the information that is provided by service providers and how the enterprise uses that information to improve over time. If the enterprise uses materials developed by outside partners, determine if the partners provide information to track engagement as described in the previous paragraph. If they do not, determine the steps that can be negotiated with the provider to remedy this situation. If an enterprise is using an external provider for phishing simulation, determine if the enterprise correlates results with awareness campaigns conducted internally or by the service provider. Systematic analysis and examination of these relationships help to determine where the enterprise may be gathering insufficient information or the wrong information, or failing to correlate the information in its possession to draw conclusions.
- **Set clear goals for improvement and track them.** For example, if an enterprise wants to see improvements of user resilience to phishing attacks increase, set a goal (e.g., 15 percent increase for the quarter) and measure improvement. Having a target helps to keep focus on specific outcomes, to understand the degree to which specific changes made are beneficial or detrimental, and to justify return on investment to stakeholders.
- **Establish or improve the governance structures in use for reporting and measurement**. The survey data suggest that enterprises are weaker than optimal in this area. Increasing the ability to gather data about the execution of awareness campaigns and the performance of those campaigns through empirical testing is likely to provide significant value to those enterprises that are lower on the maturity spectrum. One way to improve in this area is to incorporate metrics collection and reporting into awareness campaign development. For example, as enterprises develop awareness campaigns and create the materials that support that campaign, enterprises may ensure that they can measure user engagement with those materials. If an enterprise uses online or in-person user training about phishing, the enterprise may ensure that it is able to track, maintain a record of and report on user attendance. If an enterprise is sending reminder emails, the enterprise may ensure that it is tracking the open rate by users. This information is useful because it allows enterprises to determine the methods that are most effective at soliciting user engagement.

© 2019 ISACA. All Rights Reserved.

Conclusion

The ISACA survey results shows that governance and management of phishing defense can be greatly improved through better measurement and reporting. Likewise, co-sourced and service-provider relationships can directly and substantively improve how defenses perform when used and managed appropriately. Given that the data suggest a high degree of external service provider support for phishing-awareness program content and tools development and an increasing trend of using external vendors for management of phishing programs, the ability to track and measure the performance of those service providers directly affects phishing defense capability over the long term.

By understanding the maturity inherent in existing processes, understanding and evaluating systematically the service-provider relationships involved in phishing defense program, and tracking the performance of all those efforts (outsourced and otherwise), an enterprise can make improvements, track progress over time to ensure a virtuous cycle of continuous improvement and ultimately move toward better and more mature phishing defenses.

© 2019 ISACA. All Rights Reserved.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Ed Moyle
CISSP, USA

Expert Reviewers

Robin Lyons
CISA, CIA, USA

Theo Zafirakos
CISSP
CISO, Professional Services, Terranova Security, Canada

ISACA Board of Directors

Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

© 2019 ISACA. All Rights Reserved.

About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. Among those credentials, ISACA advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified in Risk and Information Systems Control™ (CRISC™), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) credentials. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About Terranova Security

Terranova Security is a global leader in security awareness training, recognized by Gartner®, with 1000+ successful phishing awareness and security awareness training programs spanning over 6 million users. Terranova Security is committed to partnering with CISOs and security professionals to help reduce human risk and support each organization with a personalized and consultative approach for phishing and awareness training needs. Uniquely positioned to help security leaders govern, manage and measure changes in behavior, Terranova Security provides true flexibility and delivery models for phishing and security awareness training. Learn more: terranovasecurity.com

DISCLAIMER

ISACA has designed and created *Phishing Defense and Governance: How to Improve User Awareness, Enhance Controls and Build Process Maturity* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2019 ISACA. All rights reserved.

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/phishing

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/

Phishing simulations are a fast and effective way to educate users and increase alertness to phishing attacks including malware, ransomware, spear phishing, whaling, CEO fraud and BEC.

BOOK YOUR PHISHING AWARENESS COACHING SESSION AND LEARN HOW TO:

- Measure user vulnerability to phishing threats
- Bolster user alertness to phishing emails
- Target the most vulnerable groups

TERRANOVA
SECURITY

Register Here For Your Free Phishing Awareness Coaching Session

TERRANOVASECURITY.COM/ISACA-PHISHING