> Dennis F. Galletta, Gregory D. Moody, Paul Benjamin Lowry, Robert Willison, Scott Boss, Yan Chen, Xin "Robert" Luo, Daniel Pienta, Peter Polak, Sebastian Schuetze, and Jason Thatcher (2024). "Balancing fear and confidence: A strategic approach to mitigating human risk in cybersecurity," *MIS Quarterly Executive* (MISQE), (accepted 10-Dec-2024).

- **Prof. Dennis F. Galletta**
  - Joseph F. Katz Graduate School of Business
  - University of Pittsburgh
  - Website: https://business.pitt.edu/professors/dennis-galletta/
  - E-mail: galletta@pitt.edu
- **Dr. Gregory D. Moody**
  - Lee Business School
  - University of Nevada, Las Vegas
  - Website: https://gmoody.faculty.unlv.edu/
  - E-mail: gregory.moody@unlv.edu
- **Prof. Paul Benjamin Lowry**
  - Pamplin College of Business, Virginia Tech, Blacksburg, USA
  - Website: https://sites.google.com/site/professorlowrypaulbenjamin/home
  - System to request Paul's articles:https://seanacademic.qualtrics.com/SE/?SID=SV_7WCaP0V7FA0GWWx
  - E-mail: Paul.Lowry.PhD@gmail.com
- **Prof. Robert Willison**
  - Xi'an Jiaotong-Liverpool University
  - Website: https://scholar.xjtlu.edu.cn/en/persons/ROBERTWILLISON
  - E-mail: robert.willison@xjtlu.edu.cn
- **Dr. Scott Boss**
  - Bentley University
  - Website: https://faculty.bentley.edu/profile/sboss
  - E-mail: sboss@bentley.edu
- **Prof. Yan Chen**
  - Department of Information Systems and Business Analytics
  - Florida International University
  - Website: https://business.fiu.edu/about/directory/profile/cheny223
  - E-mail: yachen@fiu.edu
- **Prof. Xin "Robert" Luo**
  - University of New Mexico
  - Website: https://www.unm.edu/~xinluo/

    - E-mail: xinluo@unm.edu
- **Dr. Daniel A. Pienta**
    - Haslam College of Business
    - University of Tennessee, Knoxville
    - Website: https://haslam.utk.edu/people/profile/daniel-pienta/
    - E-mail: dpienta@utk.edu
- **Dr. Peter Polak**
    - Florida International University
    - Website: https://business.fiu.edu/about/directory/profile/polakp
    - E-mail: ppolak@fiu.edu
- **Dr. Sebastian Schuetze**
    - Florida International University
    - Website: https://business.fiu.edu/about/directory/profile/schuetzs
    - E-mail: sschuetz@fiu.edu
- **Prof. Jason Thatcher**
    - Leeds School of Business
    - University of Colorado, Boulder
    - Website: https://www.colorado.edu/business/jason-bennett-thatcher
    - E-mail: jason.b.thatcher@gmail.com

“**Balancing fear and confidence: A strategic approach to mitigating human risk in cybersecurity**”

RISK IN CYBERSECURITY

Dennis F. Galletta
282 Mervis Hall
3950 Roberto & Vera Clemente Drive
Pittsburgh, PA 15260
(412) 648-1699
galletta@pitt.edu

Gregory D. Moody
BEH 329
4505 S. Maryland Parkway
Las Vegas, NV 89154
(702) 895-1365
gregory.moody@unlv.edu

Paul Benjamin Lowry
2080 Pamplin (0235)
880 West Campus Drive
Blacksburg, VA 24061
(540) 231-6596
paul.lowry.phd@gmail.com

Robert Willison
BS2123(SIP Campus-IBSS Building)
Suzhou Industrial Park
Suzhou
P.R.China 215123
+86 (0) 5120512-81889186
robert.willison@xjtlu.edu.cn

Scott Boss
Adamian Academic Center – 267
175 Forest St
Waltham, MA 02452
(781) 891-2353
sboss@bentley.edu

Yan Chen
RB 202A
11200 S.W. 8th St
Miami, FL 33199
(305) 348-6377
yachen@fiu.edu

Xin (Robert) Luo
MCM 3078
1922 Las Lomas NE
Albuquerque, NM 87106
(505) 277-8875
xinluo@unm.edu

Daniel Pienta
Haslam Business 618
1000 Volunteer Blvd
Knoxville, TN 37996
(865) 974-1753
dpienta@utk.edu

Peter Polak
11200 S.W. 8th St, RB 262A
Miami, FL 33199
(305) 348-7932
ppolak@fiu.edu

Sebastian Schuetz
11200 S.W. 8th St, RB 205A
Miami, FL 33199
(305) 348-4356
sschuetz@fiu.edu

Jason Thatcher
995 Regent Drive, Koelbel Building 419 UCB
Boulder, CO 80309
(303) 492-8397
jason.b.thatcher@gmail.com

Balancing Fear and Confidence: A Strategic Approach to Mitigating Human Risk in Cybersecurity

ABSTRACT

Despite technological advances, cybersecurity breaches persist, with human actions often being the weakest link. Educational programs and policies have been ineffective in reducing threats, as shown by rising trend data breaches and costs, averaging $9.48 million in 2023. The growing threat persists despite the plethora of tools and techniques, indicating a need for a strategic shift. Drawing on interviews with C-level IS executives and earlier experimental research, this paper advocates for greater care in warning users about security dangers, and simultaneously building their confidence in their ability to improve their cybersecurity safety. Managers must carefully balance their communications, instilling appropriate concern without causing excessive fear or negativity.

Keywords: Cybersecurity, Data Breaches, User Actions, Management Interventions, Breach Costs, Technological Vulnerabilities and Security Awareness

INTRODUCTION

The popular press and academic literature are filled with stories of breaches involving millions and even billions of customer accounts.[1] While some breaches result from unpatched and fresh system flaws, many occur by targeting "the weakest link"[2]—the user. Even the best technology can fail if an employee, consumer or social media user neglects to protect their credentials, allowing attackers to bypass technical controls.

Risky user actions have been a major focus, as highlighted by ProofPoint's 2024 large-scale "State of the Phish" report,[3] which has surveyed these behaviors since 2015. Examples include sharing passwords, not using a VPN on public wireless local networks, clicking on suspicious links or responding to urgent, unfamiliar emails. According to Proofpoint's survey, 71% of the respondents admitted to risky behavior, while 59% were unsure or denied responsibility for maintaining security, despite 85% of IT professionals believing users were aware of their role. This points to a clear knowledge and communication gap about cybersecurity threats. Vishwanath[4] describes misconceptions such as "I opened it on my phone and knew it would be safer," "What's the big deal about opening links?" and "The color and graphics were similar to our internal file sharing system." Each statement demonstrates a false sense of safety, and users need to exercise more vigilance.

Communicating the diverse threats posed by scams is crucial, but it is also important not to overwhelm users with fear, which could lead to avoidance of their systems altogether.

[1] Perlroth, N. All 3 billion Yahoo accounts were affected by 2013 attack. New York Times, October 3, 2017. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

[2] Vishwanath, A. *The weakest link: How to diagnose, detect, and defend users from phishing*. MIT Press, 2022.

[3] Proofpoint.com 2024 State of the Phish: Risky actions, real-world threats, and user resilience in an age of human-centric cybersecurity, May 22, 2024 (https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf). Their study is based on responses from 7,500 users and 1,050 security professionals, covering 15 countries. Some of the findings come from 183 million simulated phishing messages Proofpoint sent out over 12 months.

[4] Vishwanath, A. *The weakest link: How to diagnose, detect, and defend users from phishing*. MIT Press, 2022.

THE EXTENT OF THE BREACH PROBLEM

Due to factors like lack of understanding, avoidance of extra effort and carelessness, breaches continue to occur at an increasing pace. According to the Identity Theft Resource Center,[5] between 2005 and 2023, the number of reported data breaches in the U.S., the country with the highest cybercrime, has increased more than twenty-fold. In 2023 alone, 3,205 publicly reported breaches impacted 353 million individuals[6] (see Figure 1).

This equates to over eight major breaches per day. Many of the nearly 4,000 publicly traded U.S. firms valued at $250 million or more, who must report breaches due to legal requirements, are therefore likely victims of these breaches.[7]

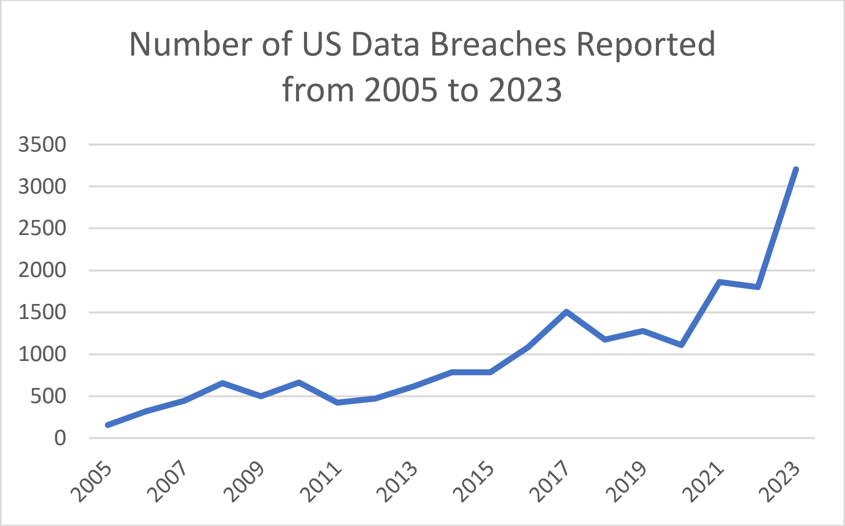


Figure 1: Number of Data Compromises in the United States from 2005-2023 (adapted from Identity Theft Resource Center, 2023[8])

Data also show a consistent increase in the cost of data breaches. In 2006, the average cost was $3.54 million per breach, rising in 16 of the past 18 years and reaching $9.48 million in 2023.[9]

[5] IdTheftCenter.org "2023 Data Breach Report, Identity Theft Resource Center, January 2024, from https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[6] Note that some individuals are reported in multiple breaches; this number exceeds the population of the United States.

[7] Frankl, M. “The Biggest Companies on the Stock Market: A Guide,” Motley Fool, November 27, 2023, available at https://www.fool.com/investing/stock-market/companies/ (retrieved June 29, 2024).

[8] IdTheftCenter.org "2023 Data Breach Report, Identity Theft Resource Center, January 2024, from https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[9] IDTheftCenter.org, pg. 13, Figure 9

Globally, cybercrime exceeded $8 trillion[10] in 2023, far surpassing the GNP of all but two Countries on Earth. For comparison purposes, Germany's GNP of $4.7 trillion pales by comparison, yet it represents the world's third-largest economy.[11]

MANY CAUSES OF BREACHES RELATE TO USERS

About 90% of all data breaches result from internal causes, including employee errors or negligence.[12] Many companies have implemented cybersecurity training programs to warn users about impacts of their various actions and inactions, but the perennial sharp rise in breaches suggests these efforts have not been fully effective. There is an apparent need to rethink how we communicate the dangers of carelessness to all users with access to a firm's systems and data.

Security and convenience often conflict.[13] Given that security controls, like authentication, add steps to frequently repeated tasks, users often see security controls as impediments to work. Business leaders, focused on productivity, also fear that security controls will reduce employee productivity, leading to a trade-off between security and performance.

The slow acceptance of multifactor authentication (MFA) illustrates this struggle. Despite the long length of time since AT&T's 1995 patent for MFA, adoption remains sluggish.[14] There is evidence of a consistent theme over several years. In 2017, 74% of IT departments adopting 2FA experienced user complaints.[15] Six years later, it was found that 73% of consumers declined to enable MFA for cryptocurrency accounts and 70% did not use MFA on social media platforms.[16]

[10] Morgan, S. (2022). Cybercrime To Cost The World 8 Trillion Annually In 2023. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[11] Estimates of the top three countries' GDP in 2024 are $28.0 trillion for the US, $18.6 trillion for China and $4.7 trillion for Germany. (source: Fund, I.I.M. GDP; Current prices. 2024. https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD).

[12] CyberAngel. Negligence Drives 90% of Data Breaches. 2024. https://cybelangel.com/negligent-data-breaches/

[13] Tam, L., Glassman, M., and Vandenwauver, M. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology* (29: 3), 2010, pp. 233-244.

[14] Daragiu, A. A review of the evolution of multi-factor authentication (MFA). typingdna.com, July 16, 2019. https://blog.typingdna.com/evolution-of-multi-factor-authentication/.

[15] Goldman, J. "74% of Organizations using two factor authentication face user complaints,"

[16] Yoneda, Yuka, "Prove identity's 2023 State of MFA Report Reveals Consumer Attitudes Towards Multi-Factor

Although smartphones have simplified MFA, users' tolerance for security improvements remains low, likely due to a lack of understanding about the importance of technical security. Also, any negative consequences, even if serious, are often not felt until much later, if ever. Users are not intentionally negligent micreants; they simply *do not fully grasp the consequences of cybersecurity carelessness.* These consequences include stolen wealth, lost jobs, or identity theft. Lack of awareness remains a significant barrier to adopting safer security practices.

While these findings focus on organizational employees, the lessons are equally relevant to e-commerce and social media platforms. Many e-commerce sites hesitate to enforce safe practices like MFA, fearing increased friction will reduce visits and sales. Social media platforms, reliant on frequent use for ad revenue, worry that MFA fatigue could lower user engagement and impact earnings. As a result, managers may opt for less secure environments to avoid frustrating or alienating users, even when MFA is available to them.[17]

How Can We Impart a Greater Understanding of Consequences?

Lack of understanding consequences is not new to society. One approach to address this was initiating "fear appeals," introduced by law enforcement agencies in the 1970s to reduce juvenile crime. The Scared Straight program took delinquent children into prisons where inmates discussed their crimes and punishments. Despite its publicity and intuitive appeal, controlled studies found little evidence of its effectiveness. One theory suggests that the program’s harshness and detailed crime discussions could inadvertently teach participants how to *commit* those crimes, inspiring the very behavior that was intended to be quashed.

Fear appeals have also been applied in health and public safety campaigns, addressing issues

Authentication,” Key findings from Prove.com (https://www.prove.com/blog/prove-identity-2023-state-of-mfa-report-consumer-attitudes-multi-factor-authentication)

[17] Abrams, L. MFA Fatigue: Hackers’ new favorite tactic in high-profile breaches. BleepingComputer.com, September 20, 2022. https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/.

like flossing, unwanted pregnancies and drunk driving. As with the law enforcement example, the outcomes were often weaker than expected. Some evidence indicates that these weak outcomes stem from failing to convince people they are vulnerable to severe consequences and neglecting to provide clear actions to avoid threats.[18] Two major ideas in self-protection motivation research emphasize that focusing solely on the severity of a threat can lead to defensive responses, discounting or dismissing the threat. It is crucial for individuals to understand their susceptibility to a threat and, perhaps more importantly, feel confident in their ability to respond to the threat.

OUR PREVIOUS STUDIES – HOW TO MOTIVATE SELF-PROTECTION BY USERS

We previously conducted and published two research articles that explored how fear appeals might work in cybersecurity.[19,20] What we learned from those two studies formed the basis of this current study, which involved interviews with executives who were intimately involved with cybersecurity. These executives responded to a set of interview questions and provided their experiences and opinions on what to do about the "weakest link" in cybersecurity.

In the first article, summarized in Appendix A-2a, participants were exposed either to severe or mild messages about the need for self-protection. Results showed that fear significantly influenced behavior, leading participants to take protective measures such as making data backups and defending against computer viruses. Our conclusion from this work was that messaging that elicited meaningful fear indeed motivated self-protection.

In the second article, summarized in Appendix A-2b, we used a newer line of thinking that

[18] Ruiter, R.A., Kessels, L.T., Peters, G.J.Y., and Kok, G. Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology* (49: 2), 2014, pp. 63-70.

[19] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly* (39: 4), 2015, pp. 837-864.

[20] Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D., and Willison, R. Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research* (32: 3), 2021, pp. 1043-1065.

considers both fear and individuals' confidence in their ability to respond. We asked employed individuals to describe how much fear they would feel in certain situations and how they would respond. Without fear, people tend not to recognize the need to act. However, as fear intensifies, individuals also require confidence in their ability to respond effectively; otherwise, they will tend to deny the existence of a threat. The more comprehensive considerations using this line of thinking provided stronger results and more strongly explained actual decisions made by our participants in response to threats. These results suggest that balancing fear and confidence is essential to foster an appropriate response to a cybersecurity threat. However, now we needed a "reality check" to see if practitioners could apply these findings in their organizations.

THE CURRENT STUDY – CISO/CIO INTERVIEWS

In search of that reality check, we turned to a group of 10 CISOs and CIOs (see Appendix A) who were actively involved with employees to motivate protective actions against cybersecurity threats. They represented diverse industries such as health care, education, technology, retail and manufacturing. We believed that they would provide valuable recommendations based on their experiences.

Our Interviews

Several authors conducted interviews with a total of ten of their acquaintances who held top cybersecurity positions. The interviews were designed to test whether our previous findings are likely to reflect actual practice (see Appendix A-2c for interview procedures). Our team asked four main questions.

1. What are the biggest barriers to protecting employees and the firm from cybersecurity risks?
2. Which tools seem to work best? Which tools are not so helpful?
3. Is it essential to instill significant fear in employees about how their actions can lead to threats?
4. How important is it to instill confidence that it is possible to defend against cyberthreats?

We wanted to know whether instilling fear is the right approach and whether employee confidence impacts their ability to avoid threats. The answers to these questions provide conclusions along with insightful quotations. Finally, we also examined patterns of agreement and disagreement among these cybersecurity experts and created a set of policy recommendations and actions for firms.

INSIGHTS FROM SECURITY EXECUTIVES

In this section, we organized our insights from the interviews into major topics that firms need to consider. We reviewed major barriers standing in the way of more effectively protecting firms, security tools that are helpful and not-so-helpful, how to instill an appropriate level of fear from the threats, and how to build self-confidence in employees.

Major Barriers Hinder Protecting Employees and the Firm from Cybersecurity Risks

Understanding barriers to protective behavior is crucial for determining effective responses. All ten participants discussed these barriers extensively. Several key issues emerged.

The size of the problem might defy traditional measurement interpretation

In one organization, the executive discovered in a fledgling phishing simulation that a password phishing email sent to 15,000 employees resulted in 1,500 clicking on it and 38 entering their passwords. While that might sound small, at a quarter of a percent of employees revealing their passwords, had these been real attacks rather than a simulation, it would have represented more than three dozen fully compromised accounts from a single phishing attack in a medium-sized enterprise. An error rate greater than zero can be of grave concern.

Policies are not enough

Organizations have used technology policies for a long time. In the 1990s, many firms quickly adopted technology policies once employees began using personal computers (PCs). For example, early policies addressed who could purchase hardware and software, what cost-justifications were needed to make those purchases, and which vendors were approved. More recently, policies were augmented by adding security-related policies forbidding such acts as reading emails addressed to others, altering company records and sharing their passwords with others. The problem is that the existence of policies alone might be ineffective:

> “Policies did not work. How often do employees look at them? NEVER.”
>
> “They are like ostriches; if they don’t know about it, then they can just do their work. We rely on software instead of policies.”

We expect too much from users

Many factors contribute to users' perceptions and assumptions. Some interviewees reported a general culture of optimism and a lack of understanding about the consequences of a breach. CISOs often expect too much from users, assuming they have expertise in facing technologically skilled adversaries. More education is needed to help users recognize attack signs, understand risks, and, most importantly, to know how to respond when encountering a threat.

> “We say they are the front line, but that is very difficult for them, as the adversary is very skilled in what they do.”

One respondent noted that there is a danger of employees believing that others are responsible for ensuring security, largely because they were trained in other fields and don’t know the proper steps to take. This indicates that not all employees realize that they can become active partners in improving security without becoming an IT expert.

Technology threats are outpacing training

Two respondents noted that training struggles to keep pace with increasingly complex cyberthreats, while one respondent highlighted that many people historically started from a place of "ignorance." Although new media is raising awareness of basic cyber risks, emerging technologies like FraudGPT and WormGPT have rapidly changed the landscape. Perpetrators are constantly improving their techniques; after years of advising users to spot grammar and spelling errors, attackers now use proofreaders and spell-checkers. A new current threat, "Pig Butchering,[21]" involves staged, “accidental” social media encounters with strangers, and faked apps used to con people out of millions of dollars. This attack is likely preventable simply by warning employees about it. Therefore, training has to be continually updated for new clever but recognizable attacks. Three other executives in our interviews back up the need for accurate and frequently updated training.

> “Cyber is changing too fast!”
>
> “Adversary is sophisticated.”
>
> “[A general guideline such as] ‘be suspicious’ doesn’t work.”

The safety mechanisms are inconvenient and make users’ jobs more difficult

Users often feel inconvenienced by MFA, leading to frustration and "MFA fatigue.” One security vendor reported that users must log in with MFA an average of 16 times daily,[22] which can lead to an employee accepting a perpetrator’s repeated request out of frustration and confusion. Another respondent told us that while most users aim for good security practices, they are overwhelmed by changes in their jobs, lingering impacts of the pandemic and the recent availability of AI apps, making it difficult to keep up with technology effectively and safely.

Another challenge is managing diverse employee needs throughout the firm. One size does not fit all; users at different levels and functions have varying skill levels, attentiveness and exposure to technology. Factory workers, for instance, lag behind office staff in security awareness. Respondents emphasized the need for tailored training:

> “We need to differentiate the shop floor versus office people—the office staff is more aware of fearful outcomes.”
>
> “The [factory workers] … are kind of aware, but they don’t use a computer all day long, so

Daniel, Lars, “The Alarming ‘Pig Butchering” Cyber Scam Costing Victims Billions—Are you at Risk?” Forbes, October 30, 2024, available at https://www.forbes.com/sites/larsdaniel/2024/10/30/this-halloween-beware-the-pig-butcher/

[22] SecureAuth. MFA Fatigue: Fighting a 2-front war. November, 2022. https://secureauthcorp.wpenginepowered.com/wp-content/uploads/2022/12/1-FINAL_MFA_Fatigue_2FrontWar_Nov2022.pdf

> they are not reinforced for their learning on these topics."

Distrust of biometrics creates a weak link

Some users distrust MFA, particularly when biometrics are used. Some of our executives noted that while fingerprints or facial scans offer convenience, skeptics fear that they could end up in the hands of companies or government agencies they do not trust. Once such private information is shared, there is no way to take it back:

> "Some people…refuse to do this – how do you get over this? Some are conspiracy theorists. Do you just block people who won't comply, or do you make exceptions?"

Most and Least Effective Tools to Improve Cybersecurity

Organizations have implemented various measures to raise awareness of threats and guide user behavior, such as warning posters, email reminders, training sessions, phishing simulations and cybersecurity policies. However, our interviewees helped us see some potential problems with training, such as boredom, obsolete topics, task overload and schedule conflicts. One respondent reported that:

> "People dreaded the annual training. Fire safety, OSHA, cyber training all at once. A TikTok ban generated attendance, but not the topic of ransomware."

Training requirements were even subverted by some of the would-be trainees. One respondent reported that annual training involving viewing several required video productions, but revealed that

> "People would open 26 windows and play them all at the same time."

Some respondents noted that well-designed posters can be effective; one respondent reported that a user provided kudos such as "Great poster this month!" However, most respondents complained that posters fall short due to the high proportion of remote workers. Opinions on the effectiveness of tools such as in-person training, policies and education varied. A possible conclusion might be that these items are sometimes done well, and sometimes done poorly. Practices that seemed to work involved gamification, keeping monthly training up to date and relevant and having phishing campaigns to provide quick feedback when employees make errors.

Rewards were often discussed by the respondents. One described the learning experience as a reward in and of itself due to feedback received during the simulations. Even when they merely receive kudos for reporting the simulated attack emails, those compliments provide recognition of their newly acquired ability to identify real phishing emails on their own. One respondent reported success in gamification of training programs, where participants pay closer attention and attend more training sessions as a result.

> "Phishing simulations seems to be one of the best - because when they fail they can be exposed to why they failed and they learn from this. They become champions about cyber."
>
> "Using the software KnowBe4 [in phishing simulations], the Phish prone phishing rate is now below 5%."

The role of the cybersecurity executive is another key issue. One executive stated that the first step is to provide a stronger case to cease being timid about imposing additional steps for employees using internal systems.

> "Five years ago, the cyber insurer didn't require anything except a signature and a check to pay the premiums. Now to be insured, a firm needs to have measures in place to fight against hacks. This helped make my case for me, shifting the blame to the insurance company."

Another important factor is the need to recognize that everyone in a firm is partly responsible for cybersecurity. Two of the respondents focused on the importance of clarifying the existence of these widespread internal responsibilities:

> "Imagine you are in high school and have a party where the house is trashed. I am like the big brother or sister that shows up and says: 'Hey, fix this up before mom and dad get here in an hour.' I'm much better than the mom and dad showing up [just] before the cops."
>
> "Security does not own the risk – business does. If you don't want to do it, fine – that's up to the business, but I will document to attest to that later."

One respondent argued for a higher level of control, discounting many of the just-discussed techniques in favor of deciding to "make the only choice the safe choice," primarily because of a vast breach several years ago that reached the news media and the SEC. They accomplished this by (1) requiring MFA for all users, even customers and (2) automating protective measures. The Finance department was an early target of these moves due to the high impact of financial breaches. Employees were suddenly required to use a password manager, and on-screen hints helped employees choose the best options for maximizing security.

In summary, feedback, rewards, and punishments were important tools to maximize employee understanding of how to recognize and avoid risks. Creating mandatory steps in company software is also powerful, essentially removing the ability of users to bypass or ignore policies. Phishing simulations were mentioned by many respondents, because they have been found to support learning over time. The benefit of easy-to-use software to make it easy to flag suspicious emails in their in-box was also mentioned by multiple respondents. Up-to-date and interactive online training with quizzes were also recommended for keeping users engaged and informed.

Instilling Significant Employee Fear About How Their Actions Can Lead to Threats

Several respondents reacted to our questions about how important it was to instill fear. Three respondents who viewed fear as very or moderately important provided compelling examples. The one reporting "Moderately Important" stated "Revealing the results of a ransomware attack that impacted everyone helped employees understand [the scale of the threat]." He added the need to be friendly and helpful without being overbearing, instilling some common-sense fear. If a stove is hot, he said, then don't touch it. "Too many lead with the boogey man, but after a while, it doesn't work because you never see the boogey man."

One respondent emphasized the need for accountability and personal consequences to keep employees from being careless. Another expressed a unique perspective: “Someday I want to ride the elephant in the parade rather than follow up with a broom,” stressing the importance of early involvement in development projects.

The single respondent who rated fear as Not at all Important made several interesting key points. Initial fear ebbs over time as safe operations become everyday practice, and early detection and resilience become the new goals. Health care workers have their own externally imposed fears due to strict regulations. While there is a danger of becoming numb to fear, those fears are imbued into the organizational culture, and those workers learned over time to be very careful. Those not involved with health data should similarly learn that lesson.

There was a spectrum of advice of fear. While one executive recommended imposing some penalties when discovering repeated errors by particular users during phishing simulations, others advocated a softer approach. One worried that it was most important just to make employees aware that “there are consequences to breaking policies.” He believed that warnings of termination too early in the learning process is “overdone” and could desensitize employees and reduce their performance. A fast feedback cycle with quick notification of errors stands a greater chance of success in the future.

> “Most of these are people just making mistakes, so we are not going to punish them - there will be no reprisals unless they were intentional.”
>
> “We just need to know about it - we need to know quickly, and then we can fix it sooner. They need to not be too scared.”

Some respondents highlighted the need for balance. One respondent described an “inverted U” relationship of fear to performance, where too little fear leads to complacency and breaches, but too much fear causes paralysis. He stressed: “You need a happy medium. Too much fear, and people stop listening; too little, and they ignore the risks.” Another respondent, skeptical of fear-based approaches, warned that excessive fear could lead to maladaptive coping, such as avoidance or ignoring the problem.

Overall, while the level of fear required varied by department, with healthcare and Finance needing more intense approaches due to stringent governmental regulations, respondents agreed that fear must be balanced with user self-confidence to avoid negative reactions. A well-calibrated fear appeal helps employees understand the threat without becoming confused or overwhelmed.

The Importance of Instilling Employee Self-Confidence that they can Block Cyberthreats

Most of our executives agreed that efficacy, the confidence to self-protect, is crucial for motivating appropriate behaviors. Of the seven asked to rate its importance, six rated it as "Extremely Important," and one as "Very Important." When asked to grade users' efficacy five years ago and today, the average grade improved from a D minus (0.5) to a B minus (2.7), after excluding factory workers, who were consistently graded an F. However, despite these gains, cybercriminals continue to outpace improvements.

A culture of “If you see something, say something,” can boost employees’ sense of empowerment. Specifically, using a “report this” button on incoming emails can stop an attack from impacting others and build efficacy. Overall, it also can identify the scope of the problem over time by assessing the dramatic decrease in clicks in phishing simulations and an increase in reports of suspicious incoming emails as employee proficiency improves.

Several respondents discussed the balance between technical complexity and clear communication. A respondent suggested using experts from within each field to explain cybersecurity in relatable terms, like a tech-savvy doctor speaking to other doctors. Three respondents praised the ease of using KnowBe4’s phishing reporting tool, where a single click allows users to report suspicious emails, fostering a high-efficacy early warning system. One of them said, "People need something simple—one-click reporting ensures phishing emails are flagged quickly."

Two respondents shared two contrasting ways in which they manage complexity. One noted that after years of being prohibited from explaining an actual breach, after a change in management he was finally permitted to show his team. Walking through the evidence with them was extremely helpful: "It was amazing—they could see and understand what could be done during a cyberattack." The other respondent emphasized making things simple, but this time to users: “We don’t talk to them about the moving parts—they just want to know if it’s working. We give them analogies, like locking a front door, so they understand why complex passwords matter.”

When asked how they could improve efficacy, a respondent remarked, “People have to feel like they can make a difference. [Simulated] phishing isn’t to make them feel bad but to help them improve without embarrassment.” Another respondent added, “We should meet them halfway—give out trophies, recognize them when they report something. Build confidence, but not so much that they stop reaching out to us.”

Overconfidence was elsewhere noted as a concern. One respondent mentioned that even when provided with free password managers, many didn’t sign up. Another added, "They think it won’t happen to them—they need superuser access, but this is exactly who we design security for. People are not as careful as they think. Even the best of us will be tricked; smart people sometimes click on dumb s***. It's not if, it’s when."

Knowledge workers typically exhibit more efficacy than non-knowledge workers, but all employees benefit from clear, easy steps for responding to threats. Good training builds confidence, but CISOs should watch for signs of security overconfidence, where employees no longer consider threats as applicable to them. Efficacy motivates adaptive responses and protective behaviors, only when a threat is perceived to exist. as confirmed by extensive research in many domains, and as we confirmed in our experimental studies that led to this current work.

Consistency of the interview responses

While there was general agreement among interviewees' responses to many of our questions, there were two areas in which the results were far less consistent: which organizational tools should be used, and how much fear needs to be imposed on users.

Differential efficacy of tools

The diversity of tools, their implementation, and each firm's unique circumstances likely could explain the inconsistency in responses about which tools work best. Training sessions generated the most diverse answers, perhaps due to large variations in content, delivery, and administration. A charismatic trainer with fresh material that includes hands-on practice in face-to-face sessions will likely achieve better results than a dull lecturer using outdated materials in a pre-recorded video. However, our respondents universally praised phishing simulations.

Another challenge with tools is the ongoing arms race between firms and perpetrators. As new security tools emerge, criminals develop ways to bypass them, prompting even newer tools. Password protection was weakened by keyloggers, phishing, and scammers posing as IT staff. MFA was introduced as a solution, but it too has vulnerabilities, such as intercepted text messages or MFA fatigue, a behavioral failure leading users to give up and just allow access to a perpetrator. It seems inevitable that firms will eventually need to move from 2FA to 3FA, perhaps incorporating biometric validation as a third factor. Just as foolproof retail theft prevention hasn't been achieved after millennia, 100% online security remains elusive. Firms must continually adapt to new threats, with some moving faster than others. For example, after a major breach, one respondent's firm mandated MFA, while most other firms still offer it as an option. Over time, such mandates may become universal.

Differential opinions of Fear: Panic versus survival

Fear, as a negative emotion, revealed significant differences in opinion among respondents. In contrast, all respondents agreed on the importance of instilling efficacy, which fosters positive emotions. We believe that three forces likely explain the variance in views on fear: (1) a desire to promote positive emotions over negative ones, (2) differing interpretations of "fear" in cybersecurity, and (3) varying beliefs about how much fear is necessary.

Our C-suite participants often emphasized positive user feedback, with some recalling moments when users praised their helpful training. Others were reluctant to induce constant fear, while some advocated for a balanced use of fear. A key takeaway is the need to differentiate between functional and emotional fear, much like Ralph Adolph's 2013 study of biological fear that found that fear can range from a *survival* instinct, like avoiding an electrical outlet, to full *panic*. Experiencing panic when walking past electrical outlets would be inappropriate and dysfunctional, making life inside any building unpleasant. But knowing enough not to insert a metal object into the outlet is based on functional, survival fear.

A cybersecurity example of constructive survival fear is encouraging users to maintain a healthy skepticism toward the "from" address in emails, letting them know that wrongdoers can easily impersonate others. By equipping users with the skills to identify the subtle clues that can identify false communications, we can prevent panic, where they become too anxious to engage at all with their inboxes. Instead, users will feel empowered to approach potential threats with confidence, improving their ability to navigate cybersecurity risks without feeling overwhelmed. Likewise, the diverse interpretations of fear in cybersecurity will likely fall somewhere along this continuum, from panic to survival preparedness.

During our study, our team realized the importance of clarifying that we aim to instill survival fear, not panic. Users must understand the serious consequences of neglecting cybersecurity threats, such as identity theft or data destruction, but panic is not the goal. The aforementioned "pig butchering" scams highlight how friendly conversations can turn into devastating financial fraud, underscoring the need for users to always approach emails with caution and suspicion.

Our experiments did not induce panic but instead provided facts to help participants make informed decisions. Phishing simulations, a form of fear appeal, allow users to make mistakes in a controlled environment and then learn from the feedback, fostering hands-on, real-world learning.

Insights from the interviews

The high-level cybersecurity professionals we interviewed held differing views on the role of fear, which we attribute to varying interpretations of the term. At one end of the spectrum, excessive fear can lead to panic, paralyzing employees and preventing them from taking any meaningful action. On the other extreme, a lack of perceived danger can result in behaviors that expose the organization to significant risks. Our interviews highlighted the importance of striking a balance: fostering a healthy, survival-focused awareness of threats to enhance an organization's resilience. However, some cautioned that fear could cast cybersecurity in a negative light or prove ineffective. One respondent argued that it's unrealistic to expect users to consistently make the right decisions, advocating instead to remove any options for lax security. For instance, strong passwords and multi-factor authentication (MFA) could be mandatory. Across the executives, there was little support for inducing panic, but much support for fostering enough fear to promote survival of the firm.

A common sentiment was that while education is crucial, training often fails to engage users. It can be difficult for them to keep up with evolving threats and understand technical issues, but boosting their confidence in their ability to combat threats is essential.

The most promising tools were phishing simulations and gamified online training. Points and leaderboards have proven effective in capturing user interest and attention. Other actions to build a more effective culture of security are also critical.

RECOMMENDATIONS

The evidence from our studies suggests a sequence of activities to enhance cybersecurity resilience, beginning with raising awareness of threats. This is followed by fostering employees' confidence in their ability to respond effectively, equipping them with specific skills through targeted training, encouraging participation via well-designed incentives, and promoting continuous firm-wide improvement.

Our findings indicate that the initial steps—awareness, building efficacy, and training—may require iteration. Starting with a general understanding of threats and the importance of efficacy, organizations can deepen employees' knowledge and skills through thoughtfully structured training programs. Once this foundation is established, the firm should implement incentive systems to sustain engagement and motivation. Finally, the organization can focus on developing its overall threat intelligence capabilities, ensuring continuous improvement and adaptability to evolving challenges.

Effective messaging is crucial for successful cybersecurity initiatives. Messaging is often users' first exposure to threats, warnings, and firm policies, making careful design essential. We argue that users aren't usually malicious but often don't fully grasp the consequences of cybersecurity carelessness. Effective security messaging should instill a healthy survival fear of threats while fostering efficacy to avoid them.

Our experiments and field interviews provide compelling evidence on some best practices in handling threat messaging. Like other daily life situations involving very high danger (e.g., driving, using electricity, or being sedentary), it's crucial to instill survival fear without causing panic. People who focus on the survival aspect of threats tend to improve their safety rather than become anxious. Empowering users to recognize and respond to threats effectively diminishes the risks. Just as many people drive while alert, avoid electrical tampering, and take walking breaks, constructive fear encourages safety without inducing paralysis.

We suggest management needs to foster a culture of constructive survival fear, enhancing users' ability to reduce threats. A continuous focus on modernization, user behavior, and company culture is necessary to balance technical challenges. Misunderstandings should be addressed through cooperation and positive learning. Promoting security awareness and responsibility, along with tailored training and positive reinforcement, can help organizations mitigate risks, protect assets, and build resilience against emerging threats.

Recommendations for specific actions, identifying fear, efficacy, training, incentives, and organization-wide threat intelligence are presented in brief in Table 1, and we will now describe them each in turn.

> "You need a happy medium. Too much fear, and people stop
> listening; too little, and they ignore the risks."

Ensure employee awareness of threats. Create a continuous, learning-focused environment to provide constructive, survival-focused fear rather than fear that would cause panic: Employees need to recognize and understand the potential dangers, but because of the complexity and continuous technological change in today's environment, such an awareness needs to be built over time through phishing simulations that can provide quick feedback, identify any individuals' or teams' vulnerabilities to phishing attacks and provide opportunities for recognition of the firm's overall progress. Clear feedback and diagnostic follow-up are essential to help users recognize a variety of attacks and learn from their mistakes. Management should track group performance rather than embarrass individuals, as punishment may induce "panic fear" and harm performance. Repeatedly dwelling on punishments and threats could also miss opportunities to reward improvement and successes.

> “Phishing reporting should be a feel-good experience where we constantly say, ‘Thank you for reporting this to the security team. Your actions are helping us get better. This helps people realize that “security is everyone’s responsibility.’”

Foster a culture of collective efficacy. Foster and reinforce users’ confidence that they can help both the organization and themselves by reporting threats or suspicious events quickly and easily. They should realize that cybersecurity is everyone’s responsibility, and therefore they should be rewarded for reporting suspicious events, representing a positive action to uncover risks. They should also share observations with others, spreading around the knowledge and at the same time providing cybersecurity professionals with early warnings about real phishing attempts. They should be made aware of their own roles, rather than instilling a feeling that it is not their responsibility to build security. Give empathetic, clear feedback when mistakes occur, encouraging a “human firewall”[23] of autonomous, security-aware teams.

> “No matter how much they try to update it, it, online training
> is always rote, dull and is always scheduled along with everything else”

Design effective training. Tailor training to fit the specific needs and skill levels of different user groups. Avoid generic, “out of the box” training that is often boring, outdated and irrelevant. Such training also misses the opportunity to address key firm-specific practices. Rather than lecturing to participants, include interactive and lively hands-on exercises, encourage participation and select trainers who engage and motivate. Stay consistent with the learning focused environment, and reward high skills, while gently pointing out to participants their errors

[23] Durcikova, A., Jensen, M. L., & Wright, R. T. (2015). Building the Human Firewall: Lessons from Organizational Anti-Phishing Initiatives. Hawaii International Conference on System Sciences, Kauai, HI, Jan (pp. 6-10).

to capitalize on rich instructional opportunities. Avoid using too much technical jargon or acronyms without taking the time to explain them.

“Incentivizing people to take precautions can be more effective than traditional training”

Introduce an incentive system. Recognize and reward improvements and evidence of proactive and useful security efforts, focusing on "carrots" rather than "sticks." Gamify their work by using leaderboards or points for top performers, motivating them without embarrassment. A point system is sometimes enough, but some employees might not pay attention without monetary incentives. Messaging should help users improve by understanding their mistakes and learning how to avoid future threats.[24] Failing to provide multiple opportunities for improvement and embarrassing some members publicly can reduce the motivation to participate.

“Education is not incredibly effective. It is made much more difficult due to constantly changing cyber attacks”

Promote threat intelligence. Threats are not static. Encourage employees to share newly discovered suspected and real threats widely, starting with cybersecurity personnel and then with others as the threats are confirmed. Promote all forms of discussions among employees, reducing knowledge gaps or silos that could leave an organization vulnerable. Scan the vulnerability horizon, exploring both new dangers and new tools and methods to protect against them. While threats keep changing over time, new tools, fortunately, are continually created and made available for adoption, and cybersecurity staff should lead the charge to keep up to date and share the knowledge immediately.

Table 1 summarizes these actionable recommendations for management, presented in the order

[24] Wright, R. T., & Thatcher, J. B. (2021, July 5). Phishing Tests Are Necessary. But They Don’t Need to Be Evil. *Harvard Business Review*.

in which each step builds on the previous one, with some iteration within the first three steps. Initially, it is crucial to ensure that employees are generally aware of cybersecurity threats. Without this foundational awareness, the subsequent step—building efficacy—will lack urgency or relevance.

Once employees understand the existence and seriousness of potential threats and recognize their role in addressing them, the next step involves exposing them to well-designed training programs. These programs should be updated regularly and effectively communicated to maintain engagement. After employees recognize the importance of their contributions, incentive systems can be introduced to enhance their motivation to continue learning and improving their skills.

Finally, the organization must continuously update and refine its strategies as threats evolve and technological solutions advance. This ensures that employees remain aware of emerging threats, feel confident in their ability to address them, and stay engaged in skill development. By fostering this ongoing cycle of awareness, capability building, and motivation, employees can contribute effectively to organizational cybersecurity while remaining informed and adaptive to new knowledge and challenges.

It is vital to ensure that any fear remains at the survival level and does not degrade into panic. Careful use of a fear appeal, effective training to raise user efficacy and proper tracking of cybersecurity tools should build user confidence and effectiveness, protecting a firm for many years against many common social engineering breaches.

Table 1: Five Key Action Points for Management

Actions	Best practices	Poor practices
Ensure employee awareness of threats	• Build a moderate level of fear so users understand the extent of possible damage that could occur with inattention • Use phishing simulations to build awareness of the wide variety of scams they could confront. • Provide quick, specific feedback to maximize understanding and recognition Report group-level results to management	• Building excessive fear that could cause users to hesitate at every turn • Repeatedly threatening users with severe punishment • Reporting individual results to management • Focusing excessively on errors and ignoring individual improvement
Foster a culture of collective efficacy	• Describe positive actions in detail and make sure users can take them quickly and effectively • Make sure they realize that they share responsibility for security • Build a team to serve as a "human firewall" that fills in any gaps left by technology alone • Encourage reporting of suspicious events to spread skills with others	• Using overly technical language, leaving users feeling helpless and hopeless • Making reporting difficult and time-consuming • Failing to emphasize the shared responsibility for cybersecurity • Missing opportunities to help team members share their knowledge with each other
Design effective training	• Make exercises concrete and practical • Treat errors as diagnostic for continuous learning • Build job-relevant skills • Use engaging, charismatic trainers • Avoid excessively technical language	• Relying on abstract concepts • Using video lectures that are boring or become obsolete • Lacking hands-on practice or follow-up • Presenting material using jargon or acronyms without defining them
Introduce an incentive system	• Provide recognition for successful skills (carrots) • Consider going beyond a point system and perhaps follow up with additional compensation • For employees who fail to improve, allow them multiple chances to improve	• Threatening with punishment (sticks) • Failing to provide multiple chances to improve • Embarrassing users publicly
Promote threat intelligence	• Encourage all forms of knowledge sharing	• Keeping knowledge in silos • Using outdated tools

	• Stay updated on emerging technologies • Identify and share new dangers widely	• Failing to scan the horizon for new technologies and tools

CONCLUSION

While technologies and policies are crucial for cybersecurity, our research highlights the significant impact of addressing the human element. Our previous studies demonstrated that focusing on equipping employees to recognize and mitigate external threats, such as phishing attacks, can yield substantial benefits. The human factor addresses two key aspects: fear of threats and efficacy—defined as employees' confidence and ability to take protective actions.

Often, users fail to identify threats or respond effectively when they do. Training programs must strike a careful balance. Avoid extreme fear that could causing panic or paralysis but at the same time, fear should be high enough to foster constructive awareness that motivates proactive behavior. This approach helps organizations recognize and mitigate risks, such as phishing messages that are designed to reveal an employee's password. If successful, such a compromise will bypass even the best technological defenses.

Insights from interviews with ten cybersecurity executives underscored the importance of cultivating a sense of urgency (fear) alongside the skills and confidence (efficacy) needed for protective action. Engaging, participative, and practical training programs, designed to be relevant and up-to-date, are critical to enhancing employees' threat awareness and response capabilities. Moreover, long-term success requires incentives that reinforce constructive behaviors and continuous learning across the organization. By prioritizing ongoing knowledge and skill development, organizations can build robust threat intelligence and resilience over time.

Appendices

A-1: INTERVIEW PARTICIPANTS

#	Industry	Position	# of Employees	Annual Revenue
1	Manufacturing	Director of IT	150	$145 million
2	Higher Education and Hospital	CISO	36,000	N/A
3	Distributor	CIO	15,000	$5 billion
4	Retailer	CISO	6,300	$11.2 billion
5	Higher Education	CISO	13,000	$1 billion
6	Government	CIO and CISO	30,000	$8 billion
7	IT Services	Security Specialist	10,000	$6.5 billion
8	Manufacturer	CISO	5,000	$3 billion
9	Government	CIO	5,000	$4 billion
10	Higher Education	CISO	1,500	$255 million

A-2A: DETAILS OF OUR FIRST SELF-PROTECTION RESEARCH STUDY

Experiments 1 and 2

In this pair of experiments, published in *MIS Quarterly*[1], we aimed to determine whether high-fear messaging had a more substantial effect on user behavior than mild messaging regarding data protection.

Experiment 1

MBA students with full-time work experience participated. Half were exposed to high-fear messaging about data loss ("high" fear group), while the other half received a mild and humorous message suggesting the importance of data backups ("low" fear group).

Unlike many studies, we measured intentions and actual behavior, verified through system logs and self-reports. Participants used their own computers, making the threat feel more personal and relevant. Both groups were analyzed using Protection Motivation Theory (PMT) [2], which includes:

- Severity: Perception of threat seriousness.
- Susceptibility: Perception of personal vulnerability.
- Efficacy: Confidence in avoiding the threat.
- Response cost: Low effort, difficulty and execution time for protective actions.
- Fear: Personally relevant threats generate fear.

Experiment 2

Undergraduate students with an average of six months of experience participated by accessing a copy of a well-known camera review site on the experimenters' server. While performing a task on the site, participants were interrupted by a virus warning message. The high-fear group were threatened severe consequences if ignored, while the low-fear group saw a message about benign effects. We tracked who ignored the warning and who chose to quarantine or remove the virus.

As we predicted, the high-fear groups showed much stronger responses to their fear appeal. Using all of the measures, the "full" PMT model explained nearly 80% of their actual behavior—significantly better than previous studies that only measured intentions or used incomplete models.

[1] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., and Polak, P. What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly* (39: 4), 2015, pp. 837-864.

[2] Rogers, R.W., and Prentice-Dunn, S. Protection motivation theory. In, Gochman, D.S., (ed.), *Handbook of Health Behavior Research I: Personal and Social Determinants*, New York, NY: Plenum Press, 1997, pp. 113-132.

A-2B: DETAILS OF OUR SECOND SELF-PROTECTION RESEARCH STUDY

Experiments 3 and 4

In this pair of experiments, published in *Information Systems Research*[3], we explored a more comprehensive approach to fear appeals, focusing on both fear and participants' confidence in their ability to overcome a threat. The study utilized the *Extended Parallel Process Model* (EPPM) [4,5], which introduced the idea that fear does not simply lead to a "response versus no response" outcome. Instead, users follow one of three distinct paths in making their decisions, as outlined in Table 1.

Table 1: Three different Paths in the EPPM (Adopted from Witte[5,6])

Threat	Efficacy	Level and role of fear	Outcome
Low	Low/high	No or low fear (no role)	A. **No response**: no coping appraisal or further processing—threat ignored
High	High	High/moderate fear mediated by threat (indirect role in danger control)	B. **Danger control** (adaptive coping): positive intentions to protect (i.e., protection motivation)
High	Low	Extreme/high/moderate fear/threat mediated by fear (direct role in fear control)	C. **Fear control** (maladaptive coping): avoidance, reactance, negative intentions, etc.

The experiments confirmed most of our predictions:

- High threats lead to high fear.
- Threat, efficacy, and fear strongly predict policy compliance and non-compliance.
- Low efficacy and high fear did not always result in fear control, but efficacy generally led to compliance
- Danger control was triggered when both efficacy and fear were high.
- "Rewards" for ignoring policy and high response costs contributed to avoidance and non-compliance intentions.

[3] Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D., and Willison, R. Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research* (32: 3), 2021, pp. 1043-1065.

[4] Witte, K. Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs* (59: 4), 1992, pp. 329-349.

[5] Witte, K., Cameron, A., McKeon, J.K., and Berkowitz, J.M. Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication* (1: 4), 1996, pp. 317-342.

A-2C: INTERVIEW PROCEDURES FOR OUR PRACTITIONER STUDY

Ten senior-level cybersecurity practitioners were selected from the authors' personal contacts. The group included three CIOs, six CISOs, one IT Director, and one senior cybersecurity analyst (one participant served in both CISO and CIO roles). The sample spanned the U.S., ensuring geographic diversity.

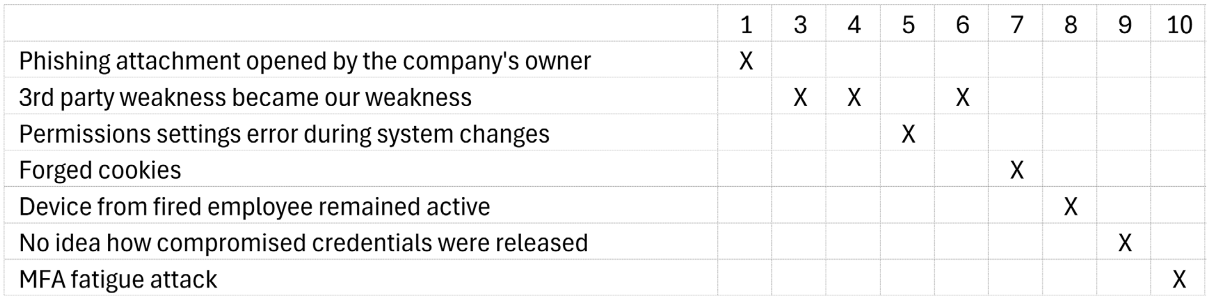
To encourage candid responses, we assured anonymity, promising not to share firm or participant names. Firm sizes ranged from $145 million in annual sales with 150 employees to companies with revenues in the low billions. One respondent represented a state government agency, reporting funding rather than sales. The average revenue was $4.17 billion, and the average headcount was 17,865. Participants came from various industries: distribution, retail, education, healthcare, manufacturing, technology, and government.

The interviews, averaging one hour each, were not recorded. Researchers paraphrased the responses and confirmed with participants that the excerpts accurately reflected their intent or wording. The final draft of the submission was sent to the interviewees for final checking. No errors or misunderstandings were reported.

APPENDIX B: SUPPLEMENTARY FINDINGS

Before concluding the interviews, we asked each respondent to describe their most recent significant breach and how it occurred. All but Respondent 2 provided details, which are summarized in Table 1. The table also offers context for the organizations each respondent represents.

Table B-1: Most Recent Significant Breach Suffered by Each Respondent



	1	3	4	5	6	7	8	9	10
Phishing attachment opened by the company's owner	X								
3rd party weakness became our weakness		X	X		X				
Permissions settings error during system changes				X					
Forged cookies						X			
Device from fired employee remained active							X		
No idea how compromised credentials were released								X	
MFA fatigue attack									X

The diversity of breaches is striking, suggesting that management cannot limit their vigilance to a few potential causes. Perpetrators continually devise new schemes targeting numerous weak points, and top management must recognize the scope of this threat.