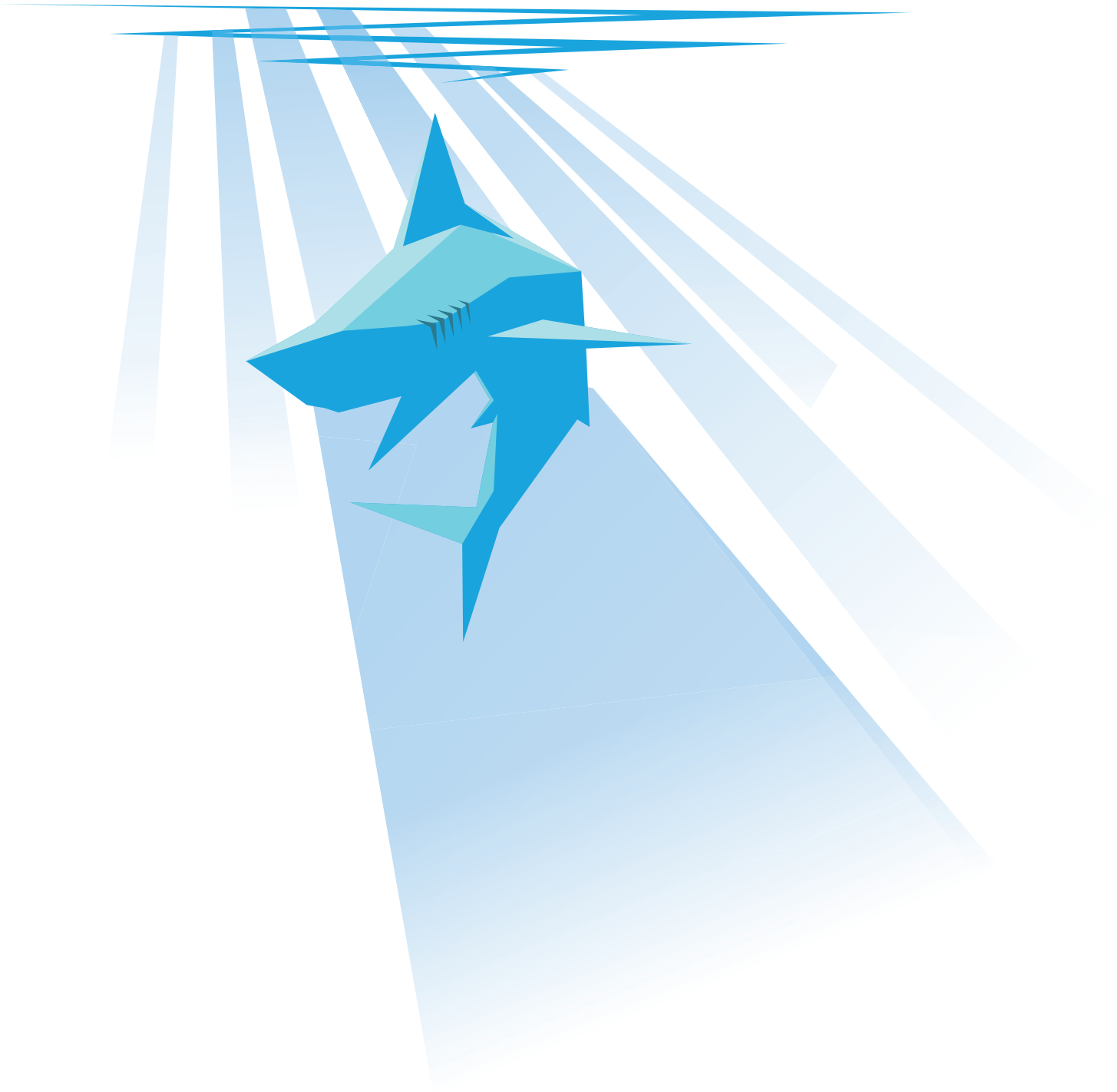
BDO DIGITAL

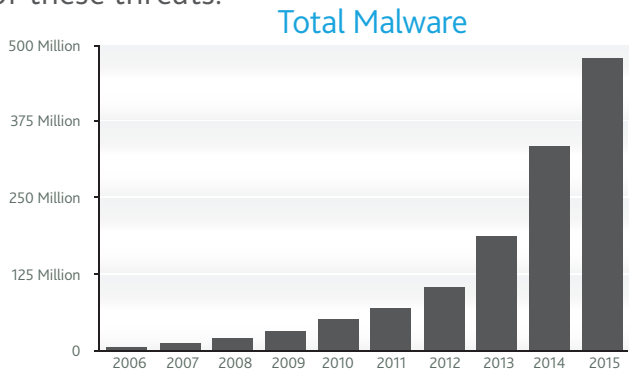
PHISHING for an Unwitting Accomplice

THE WEAKEST LINK IN YOUR CYBER SECURITY



The continued evolution of technology presents new opportunities for growth in the mid-market, giving organizations the ability to exponentially scale their operations and compete with larger enterprises. However, these new opportunities also produce a great deal of risk, as cyber-theft continues to threaten organizations of all sizes. If you think you aren't a target, then think again! Every organization has information valuable to attackers including customer names, user credentials, credit card information, and social security numbers. Unfortunately, a majority of these attacks go undetected as businesses of all sizes struggle to stay ahead of these threats.

Cyber-crime has steadily been on the rise, as new advancements in technology open new methods to exploit weaknesses to compromise your sensitive information. In 2015, over 140 million unique pieces of new malware were registered, fueling a steady year-over-year increase that began to significantly gain momentum in 2007. From 2014 to 2015, 38% more security incidents were detected across organizations of all sizes. For mid-size companies specif ically, that number increased by 64%.[ii]



Source: AV-TEST GmbH, www.av-test.org

2014-2015

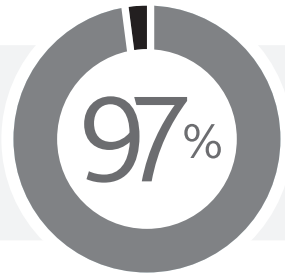
64% increase in security incidents in the mid-market

Today's cyber-attackers have developed proven methods to gain access to your network and data. Attackers, like cyber-security professionals, examine trends to determine the most viable methods to exploit your information and countless studies have all pointed to one result. The vast majority of attackers enter networks through the same vulnerable channel using the same proven method – exploiting **your users** via a phishing email.

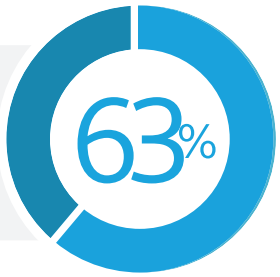
PHISHING ATTACKS & YOUR USERS

Attackers are looking for the path of least resistance and most often their opportunity comes when your users mistakenly help facilitate their inf iltration. A security study released by Verizon found that 90% of all cyber-attacks start with a phishing email. In this study, a small phishing campaign of only 10 emails hooked at least one victim nine out of ten times. The study showed that on average, 23% of these emails were opened and 11% of those tested even took the extra step of downloading an attachment. Why are these users so susceptible to these phishing schemes? A 2015 Intel Security Study discovered that threat identif ication is likely the key factor, as 97% of the users tested in the study could not identify a phishing email.[iiiiv]

of security incidents involve human error



of users can't spot a phishing email



have compromised or forgotten a password

Sources: Georgia Institute of Technology, IBM, Intel

Time is truly against IT teams once a phishing attack is perpetrated. On average, the time between a phishing email being sent and the first person clicking on the link is 1 minute and 22 seconds. Considering the amount of attacks that go unnoticed, that window simply isn't enough time to react to the threat. **This makes empowering users to recognize threats and educating them on security protocols one of the most important components to any security strategy.** All it takes is one click to compromise your entire network. [v]

Attack Models

Cyber-attackers use a variety of methods to structure an attack depending on their end goal and the perceived value of their targets. Generally speaking, these attacks fall into either basic, 'wide net' phishing or advanced 'spear' phishing. The key differences lie in the effort required to execute the attack, the size and profile of the target, and the availability of intelligence on the potential victim that the attacker can gain access to prior to the attack. Whatever the method, all attacks have the shared goal of manipulating victims into exposing their sensitive information.

Wide Net (Basic)

The Wide Net, or basic attack is the most common model. It is less targeted, but also easier to execute at a larger scale. With wide net attacks, the perpetrators operate on a broad scale and attempt to appeal to a mass audience. While these attacks are easier for end users to identify, they are continually evolving and becoming more sophisticated and increasingly diff icult to detect.

Mass SPAM Email Sent to a Large Group of Users

Volunteers Information or a Malicious File Download From a Link

User's System is Infected with Malware or Remote Access Trojan

1. The attack begins with a mass spam email sent indiscriminately to a large list of contacts. These emails are often disguised as operational communications from reputable sources that many people use such as PayPal, Facebook, or a delivery service like UPS or FedEx. The email will contain a link or a call-to-action designed to turn recipients into accomplices.

2. The link will direct victims to a semi-professional looking website, to maintain the illusion of legitimacy. One method attackers can use is to prompt users to enter login credentials or other sensitive information on this website. However, a single click is all the attacker needs, as simply clicking on the link can trigger a malicious Trojan horse.

3. The attacker can test login credentials on multiple destinations as users often keep the same credentials across accounts. In the event of a malicious fsaved keychains or access sensitive information on users' local or shared drives.

Spear Phishing (Advanced)

Spear Phishing, or the advanced attack model, is more complex and targeted. In Spear Phishing, hackers invest time to collect information on their targets prior to launching their attack, to increase the likelihood of deceiving recipients. In many cases, this information can be found on social networks or from data gathered in a previous attack. While this model requires more effort per attack, it typically has a higher success rate.

1. Attackers gather intelligence on their targets through social platforms such as Twitter, Facebook, and LinkedIn. They often will look to target victims who have access to sensitive company data or systems. Attackers may also follow their victims' social trail to determine their coworkers, friends or other trusted contacts.

2. A lookalike domain that is relevant to the target is registered. The lookalike domain will look similar to the actual destination, possibly replacing an "i" with an "l" or another subtle change. Some examples of the domains recreated include insurance providers, frequently used shipping companies, or even the target's company website. Attackers will use these domains to set up falsifsometimes impersonating themselves as service providers, colleagues, clients or superiors.

3. The attacker sends a personalized email to each target with a call-to-action to click on a link or download an attachment. The destinations for these links are disguised as relevant information such as reviewing insurance information, 401k changes, or shipping confirmations. Some attackers may attempt to execute wire transfer fraud at this at this stage, depending on the access their intended target may have to f inancial transaction authorization.

4. Once the user clicks on the link, they are directed to an offpretense that the phishing email was legitimate. On the website, the attacker may attempt to obtain credentials, but more often their goal is to trigger a download which may be disguised as a routine download like a Flash, Java or other software update. Often, it will not even require the user to opt-in to the download and can occur in the background in a manner that is not obvious to the end user. After the file is downloaded, their system is infected with malware or a remote access Trojan horse.

5. The malware grants the attacker access to any sensitive information contained in emails, on local drives, or in any shared network drives that the user may have access. Typically targets in spear phishing are targeted because they are most likely to have access to sensitive company materials.

6. The hacker uses this access to collect sensitive information from the end user. Attackers are also able to remove evidence that a breach even occurred before they complete their attack.

Once the hacker has your data, the attack can go in a variety of directions depending on what data they were able to access. A cyber-criminal might levy fraudulent charges extracted from saved payment information, generate falsified credit lines from social security numbers, initiate wire transfers from accounting data, use customer data to perform subsequent attacks, or even perpetrate extortion scams locking organizations out of their own data until they pay a ransom to retrieve it.

Types of 'Bait'

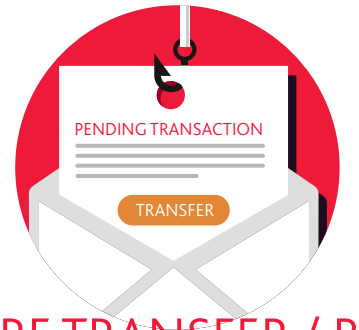
The 'bait' in phishing emails can take a variety of forms and leverage different tactics to manipulate end users into exposing their sensitive information. The types of attacks below represent some of the more relevant and common 'bait' BDO Digital has encountered most in mid-market organizations.

MALWARE BASED

The goal of these emails is to trigger a download of malicious software onto the users' system. These emails are successful when a user clicks the call-to-action or downloads an attachment.

CREDENTIAL

These attacks, disguised as operational "password resets," attempt to trick users into entering their credentials into fake web forms as many users use the same passwords across accounts.



WIRE TRANSFER / BEC

These attacks impersonate the attacker as a CEO, CFO, or other company authority and attempt to get the victims to initiate wire transfers, often with a sense of urgency.

I'M NOT A BIG PHISH, SO I'M NOT AT RISK

While data breaches in larger organizations like Sony and Target make the headlines, what is often overlooked is that hackers are attacking organizations of all sizes, arguably causing an even greater impact to the bottom line of small and mid-market organizations. These attacks are relatively low-cost and low-risk to execute, and cyber-criminals use eff icient, repeatable methods to cast a wide net with high frequency. Incidents detected by midsize U.S. organizations have led to an estimated average f inancial loss of $1.8 million per company annually. The true loss is likely far higher, considering a majority of attacks (up to 70%) go undetected.

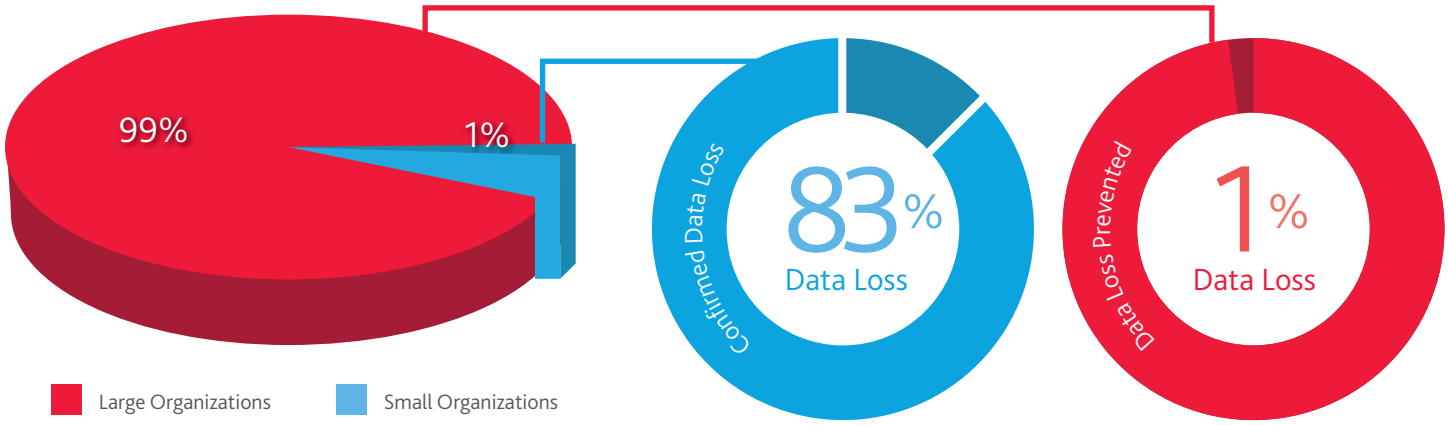
$1.8M

Average Financial Loss Detected By U.S. Organizations Annually

In Verizon's 2015 Data Breach Investigation Report, only 1.3% of what is classified as "small businesses" reported a security incident. Interestingly, these small organizations reported that 83% resulted in confcompared to larger organizations who reported that they only lost data in 1% of their attempted attacks.

Total Reported Security Incidents

Confirmed Data Loss



While larger organizations are self-reporting a far higher total number of security incidents, small organizations have less success fending them off without data loss, indicating they may not be recognizing threats until it is too late.

Cursory review of the data may indicate that smaller organizations have a lower risk of attack, as their total number of reported security incidents are miniscule compared to larger organization's reports. However, it is important to distinguish that all of the data in this study is self-reported. Paired with the confstatistics, a more troubling picture is painted for these smaller organizations. While larger organizations are reporting a higher incidence, they are fending off 9 out of 10 security threats without the loss of data. By contrast, smaller organizations are fending off only 17% of their self-reported security incidents. In fact, even though larger organizations are reporting nearly 73 times more incidents, they still have a smaller net total of irmed data loss. So perhaps **that they are unable to register these incidents as a threat until it is far too late** mitigate the risk to the business.

BDO Digital's mid-market clients have reported losses of over $100,000 to CEO/CFO wire phishing. Of the organizations targeted by phishing campaigns, 46% had under 500 employees. The reality is that mid-size businesses face the same risks, and in the absence of a specialized cyber-security staff, they face an uphill battle to address these challenges. Small and mid-market businesses are at a greater risk than larger organizations as they have more vulnerabilities to expose. Roughly **60% of small businesses close within six months of a cyber-attack.**[ix] While consequences of a data breach in a large enterprise might cost jobs and revenue, a serious data breach in a small to mid-market organization could jeopardize the future of the entire business.

WHAT STEPS CAN I TAKE TO PROTECT MY DATA?

In today's environment, the question isn't if you are going to be attacked, it's when. Developing a mature security plan is to recognize that cyber security isn't just an "IT problem." Security should be an initiative that stretches across the entire organization. Successful threat mitigation plans take a top-down approach, especially when you consider that prime Spear Phishing targets reside in the C-Suite.

> "49% of companies do not perform employee security awareness training…their annual losses are four times greater than those that do have a training process in place"
>
> - Georgia Institute of Technology

While developing safeguards to protect your data is important, having a risk mitigation plan in place when the inevitable attack occurs is critical. A systematic, holistic approach that leverages not only technology, but behavioral training, will ultimately produce the best results. While technology can help to secure your information, a foundation must be in place to make it effective. Security awareness training is one of the most impactful steps you can take to transform security from an "IT problem" to a business-wide initiative that stretches across the organization.

Customized Security Solutions

Understanding the risk your users present to your security is a key step in determining the gaps to address to protect your organization. BDO Digital can partner with you to develop a customized security awareness program that educates your users and turns them into your first line of defense in a cyber-attack. While our solutions and partnerships are tailored to meet the needs of each organization, our security awareness training follows a general framework:

Assessment & Testing

BDO Digital leverages our team of security experts to 'pressure test' your organization by safely simulating real-world social engineering and phishing attacks. These tests will provide a baseline for assessing **your users'** ability to spot a potential threat.

Risk Analysis

Which scams are your users falling victim to? BDO Digital reviews the results of the assessment and develops a comprehensive report that lays out your organization's opportunities to improve through user awareness training. Which areas of the business represent the highest risk? **We can also determine the potential information that could have been compromised in an actual attack.**

User Awareness Training

BDO Digital will create a comprehensive training program that is unique to your business, prioritizes the protection of your most valuable data, understands your security compliance policies and addresses the key risks determined in the evaluation. The training will educate users how to spot phishing emails, identify red flags, and participate in the threat escalation and mitigation process. BDO Digital also takes the program across the finish line by owning the rollout and user adoption of the new security protocols. BDO Digital can host remote training for off-site personnel, create online quizzes to test training, and generate reports for audits or compliance purposes. Finally, we continually test the efficacy of the program and keep our partners involved in results tracking throughout the process.

Holistic Approach

While behavioral training is a key component, it is only one gap that needs to be addressed in a comprehensive security program. BDO Digital's Information Security Practice works closely with each of our partners to understand the nuances of your business to optimize our security recommendations. Our suite of security solutions include action plans concentrated on behavioral training, prioritization of key data, and systematic regular testing.

TECHNICAL SECURITY

- Vulnerability Assessment
- Penetration Testing
- Web Application Testing
- Security Infrastructure Implementation
- Business Continuity & Disaster Recovery
- Access Control & Management

RISK

- Virtual CISO
- Security Assessment
- Policy Design & Review
- Control Analysis
- Security Program Development
- Threat Profiling
- Phishing Campaigns
- User Awareness

COMPLIANCE

- PCI Preparation
- HIPAA Readiness Review
- ISO 27001 / 27002
- Gap Analysis
- Standards & Framework Design

MANAGED SERVICES

- Managed & Monitored Firewall
- Virtual CIO
- Security Log Review
- IPS / IDS Tuning / Management
- Managed Logging
- Managed Vulnerability Scanning
- Next Generation Firewall
- Web Application Firewall
- Advanced Threat Detection / Prevention
- Threat Intelligence Bulletins

CERTIFICATIONS

CISSP ISSMP CISM GPEN C|EH CCNA CCNP

BDO Digital provides a wide range of solutions from infrastructure and security to business intelligence, software solutions, and an industry-leading Managed IT Services practice. Across all of these solutions, our approach is to become your strategic partner, understand your business and your priorities, and develop a solution that works for you to achieve success.

ABOUT BDO DIGITAL

BDO Digital is your leading provider of IT services and technology solutions. For more than 35 years, BDO Digital has excelled at helping Midwest organizations harness technology that drives innovation and accelerates business transformation. We specialize in business technology solutions that match the needs of midmarket organizations, including Managed IT Services, Infrastructure Solutions, Software Solutions and Digital Marketing. Our focus is to identify our clients' business goals first, then leverage our team of business and technology experts and full stack of IT capabilities to partner in their success. We are the experts in deploying technology solutions, but truly what we do for our partners is deploy value.

To learn more, contact us at bdo.com/digital