Fortune 100 Company Executive Digital Risk Report

DATE: 09/20/20

1. SUMMARY

PiiQ Risk conducted a complete Social Media Risk Assessment of five hundred Fortune100 company executives. PiiQ Risk identified available social media accounts for each executive across LinkedIn, Facebook, Twitter, and Instagram and then applied PiiQ's Risks analysis and scoring. The data included in this report represents the cumulative percentages of some of the highest risk factor occurrences for all 500 executives.

Social Engineering (Phishing) based attacks are currently the primary threat to organizations within an increase in frequency by 667% since January 2020[1]. The average data breach now costing US companies roughly $11M dollars[2]. The problem is current corporate security practices and technologies provide little guidance and protection for the personal digital footprint of their employees, a footprint that is providing the information and paths necessary for individual and corporate cyber exploitation.

The results of our assessment are startling, even the most at-risk individuals for the highest value companies in the US have significant lapses in personal and corporate security best practices that are putting companies at risk. Companies can no longer afford to overlook employee personal digital and social security best practices as part of their overall security strategy. In order to address this gap, companies need to adopt more actionable social media use policies and implement continual assessments of employee personal information exposure as it effects corporate risk for data breaches.

2. CORPORATE DIGITAL RISKS

Individuals' digital footprint has significantly increased in the last ten years, as online services create business opportunity and convenience. The multitude of sites and services that have some portion of our personal information have become difficult to manage, far worse is the inability to understand and mitigate the combined risks of our aggregated personal information and activities across these various sources. Unfortunately corporate digital or social media use policies have not evolved to provide effective and actionable guidelines that properly protect individuals and organizations. For that reason, PiiQ Risk has produced a much more detailed **Corporate Social Media Use Policy Template**. https://www.piiqmedia.com/resources/cyber-security-policies

In addition, corporate policies on employee use of personal devices for work place communications further complicate corporate security best practices. Over 60% of employees now use their personal smartphone for work purposes[3]. The security risks created by Bring Your Own Device (BYOD) policies has been largely accepted because of the personal convenience and cost benefit to business operations. We now have a set of devices that are used to access both personal services as well as corporate resources.

Further complicating security efforts is the massive shift in remote working brought on by the COVID-19 pandemic. Roughly 88% of organizations now either encourage or require employees to work from home[4]. Those same blended devices now sit predominately

outside the traditional corporate network and perimeter security infrastructure. It is a perfect combination of risk factors that greatly favor criminal activities to access corporate resources. In fact, IBM Security Study Finds, *"More than 80% of respondents either rarely or never worked from home prior to the pandemic, and in turn, more than half are now doing so with no new security policies to help guide them"*[5].

3. RESEARCH FINDINGS

PiiQ Risk has developed social media risk scoring that takes into account the combination of individual risk factors that collectively create more significant paths of exploitation. In our analysis **the average PQ-RISK score was 183.84 out of 300, which represents a serious risk of information exposure and exploitation based on the public information that was available and analyzed.** One of the lowest risk scoring companies, IBM, scored an average of 148 representing still, a moderate risk to the company. Even for the best scoring companies, there are identified vulnerabilities across personal relationships, attributes, content, and technical factors that can be compromised by attackers. Meaning, even if your individual risk scores are moderate, to a focused attacker there is enough information publicly available to launch a successful social engineering attack. It would just take a little more work.

Table 1 lists the percentages of occurrence for 11 of the risk factors PiiQ Risk measures. Each of these risk factors pose a threat individually, but combined create enough personal context that poses critical personal and corporate risk of exploitation.

The first requirement by most attackers is to identify persons of interest based on an association with a company, job title, or other organization based on membership or interest. Listing specific employment or membership information should be avoided if possible, but often we find companies encourage employees, especially senior ones to publicly associate themselves to the company and simultaneously promote themselves and their company. In these cases, it is even more important for those individuals to ensure their other publicly available digital information is assessed for exploitation risk and monitored. In our analysis the majority of executives publicly list this information, but additionally publicly exposed relationships around employment and interests are also accessible for most executives, providing context that is more easily exploitable.

The next step for attackers is to obtain means of communication, such as an email address, phone number, or social media account. In our analysis we were able to identify a personal email address for 61% of executives and a business email address for 98% of executives. In addition more than 61% had three or more social media profiles that were easily discoverable. We found that 32% of executives have email accounts that do not have proper DMARC/DKIM/SPF records set which allows attackers to more easily impersonate valid email accounts making it more difficult for a potential victim to assess and detect malicious from authentic emails.

The final step is to build context around the target individual(s), to identify close friends, colleagues and close personal interests and activities that can be used to build context for a tailored spear phishing attack. The more information a threat actor has access to, the more contextualized the attack, increasing the likelihood of compromising the target individual(s). Relationships not only provide individuals that can be impersonated but they also expose shared attributes that provide relationship context. From our analysis the overwhelming majority of executives have exposed relationships that share employment, education, and interests.

EXPOSED PII	ASSOCIATED RISK	%
Discoverable email accounts attached to personal social media accounts	Emails remain the main conduit for phishing. Being able to recover emails because of proper name usage, username re-use.	67%
Business email accounts attached to personal social media accounts.	A business email should never be associated with personal internet services, such as social media. It opens up a larger set of responses through business email that needs to be policed.	23%
Emails exposed in breaches in last 12 months	Email breaches expose personal information, including email addresses that otherwise may not be easily accessible.	74%
Business Emails exposed in breaches in last 12 months	Business email breaches pose a direct threat to organizations especially if combined with password compromises since a majority of individuals use passwords across multiple sites and services.	62%
Passwords exposed in data breaches	Breaches that contain passwords pose serious risk to the individual and corporate mostly due to password reuse across services.	44%
Email accounts without properly configured or set DMARC/DKIM/SPF records.	DMARC/DKIM/SPF provide DNS and email security features that make it far more difficult for attackers to impersonate trusted domains. Not having these properly set makes it much more difficult for individuals to detect phishing emails.	32%
Exposed relationships that divulge a shared education	Personal relationships can expose key personal attributes as well as providing context. This allows an attacker to impersonate someone and have necessary context to fool the victim.	97%
Exposed relationships that divulge shared employment	Personal relationships can expose key personal attributes as well as providing context around the relationship allowing an attack to have a person to impersonate and the context around the relationship.	99%

EXPOSED PII	ASSOCIATED RISK	%
Exposed relationships that expose shared interests	Personal relationships can expose key personal attributes as well as providing context around the relationship allowing an attack to have a person to impersonate and the context around the relationship.	99%
Publicly exposed location check-ins	Location information poses both digital and physical risks to individuals as it provides information on frequented locations as well as locations of interest. Using location information in spear phishing campaigns, such as restaurants, shops is often successful because of its close personal connection.	35%
Open friends lists on Facebook	Publicly open friends lists allow an attack to more easily build context around a victim and provides an immense amount of information regarding relationships which would be used by attacks to impersonate connections.	43%

Table 1: Fortune 100 Executives Social Media Risk Factors

4. SUMMARY

Given the information results of PiiQ Risk's research it is clear how exposed corporations are to spear phishing related attacks targeting company executives. The necessary vulnerability elements exist, creating an extremely difficult environment for corporate security teams to effectively protect corporate executives and information systems. Watching the trend in targeted attacks on employees to gain access to corporate information systems, it is clearly only a matter of time attackers develop automated systems to collect this information and develop more advanced automated exploitation systems. Phishing and spear phishing detection systems continue to evolve to novel attacks and yet companies are increasingly compromised. The only means to effectively reduce risk to organizations against future advanced attacks is to adopt more detailed Corporate Social Media Use guidelines, incorporate employee social media risk assessments and provide more tailored awareness training for employees, especially to those at higher risk.

5. REFERENCES

1. Insider Breach Costs Rise to $8.7M. https://www.infosecurity-magazine.com/news/insider-breach-costs-rise-to-87m/
2. Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020. https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020
3. The Future of BYOD: Statistics, Predictions, and Best Practices To Prep For The Future. https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#68d44ad61f30
4. 15 Surprising Stats on the Shift to Remote Work due to COVID-19. https://www.riverbed.com/blogs/15-surprising-stats-on-remote-work-due-to-covid-19.html
5. IBM Security Study Finds Employees New to Working From Home Pose Security Risk. https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk