Society for New Communications Research

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

SNCR 2020 Series
Exploring New Communications Tools and Technologies

The State of Digital and Social Media Risk Management

2017 Edition

By Jen McClure and Alex Parkinson

Companies face a growing number of risks from digital and social media and are challenged to effectively and comprehensively manage them. The fallout from not properly managing digital risk can be significant, as witnessed by the numerous recent hacks on all types of organizations from government institutions to companies of all types, including media and entertainment companies, retailers, and financial institutions. This *SNCR 2020* article suggests that although digital governance teams and Digital Centers of Excellence are becoming common oversight structures and many organizations have policies, procedures, and programs to manage traditional IT security risks, most do not yet have fully optimized, managed, and resourced processes and programs to manage new and growing types of digital and social media risks.

This *SNCR 2020* article is based on the key findings of the State of Digital Risk Management study, conducted by JEM Consulting & Advisory Services in early 2017.

SNCR-005 | OCTOBER 2017 | Subscribe for free at www.conferenceboard.org/sncrblog

Digital risk has yet again been front page news recently. As just one example, Atlanta-based credit reporting company Equifax faced a series of breaches from May 13 through July 30 this year that resulted in the personal information of more than 140 million American consumers, including social security numbers, being accessed by hackers.[1] Equifax has blamed the breach on a web-application vulnerability that had a patch available in March—two months before the attack.[2] The company continues to suffer from its misstep, with some experts suggesting it will not survive as a result.[3] Fallout (at the time of publication) includes:[4]

- Approximately $4 billion loss in market capitalization
- A Congressional investigation
- CEO Richard Smith stepping down
- Probe by the Federal Trade Commission
- At least 70 class-action lawsuits (and potentially more to come)
- Resignations of chief information officer and chief security officer.

Among many issues, the incident calls into question Equifax's processes and policies related to digital risk management, which is a constantly evolving issue that requires detailed attention and sophisticated management responses.

Challenges with Digital Risk Management

Organizations face a wide, complex, and increasing number of digital and social media risks as they enter an increasingly digital business landscape, but it appears that the most entrenched issues continue to worry companies most.

A majority of companies acknowledged that malware (51.7 percent) and email security (50.2 percent) present the biggest challenge when it comes to digital risk management. Both malware and issues related to email hacking have afflicted business for some time and these middling percentages tell two stories:

1. On the negative side, both continue to be popular ways for hackers to infiltrate organizations' security. The popularity and success of malware attacks has resulted in a robust underground industry that updates and releases new malware often; and while email continues to be the most popular communications tool in business, the payoff for infiltrating those systems will continue to be appealing for hackers.
2. On the positive side, organizations have had long enough to develop sound policies, procedures and programs to defend themselves from such attacks, although the consistency of attacks demands constant vigilance (see more information below).

Companies spread themselves consistently in terms of identifying other risk areas that posed the biggest challenge—percentages ranged from 21.2 percent for mobile to 39.4 percent for cloud-based applications, with 11 other risk areas in between. The percentages suggest that companies are spreading their attention across an ever-growing range and number of digital risks stemming from web, mobile, and social media.

Table 1

What are the biggest challenges you currently face with regard to your digital risk management?

Risk areas	Percent
Malware	51.7%
Email security	50.2
Cloud-based applications	39.4
Breaches	36.9
Data collection storage and management	36.0
Brand fraud	35.5
Website security	35.5
Backend systems	32.0
Phishing	32.0
Digital trolls	31.0
Bots	29.6
Denial of service attacks	29.6
Social media accounts	29.6
Imposter social media accounts	25.1
Mobile	21.2

Source: JEM Consulting, 2017

Managing traditional IT security and digital risk

As suggested above, most organizations have established policies, procedures and programs to manage more traditional IT security and digital risk effectively. For example, the vast majority of companies have anti-virus measures that cover all system areas; most companies have performed an external and internal security reviews in the past 12 months; companies also tend to have information security policies that are periodically reviewed and updated; and three-quarters of companies have a formal process to report and handle security incidents, weaknesses and software issues.

These are just a handful of examples among a host of other findings regarding traditional security practices that are widely adopted by companies, as outlined in Charts 1–12 (pages 4–5).

Chart 1

Does your organization have antivirus measures in place?

If yes, do these cover all system areas, including live and development environments, desktops, servers, gateways, laptops and other mobile devices?

Chart 2

Has your organization performed any external or internal security reviews in the past 12 months?

Chart 3

Does an information security policy exist?

If yes, are periodic reviews and updates of the policy performed?

Chart 4

Does your organization have a privacy policy?

If yes, is your privacy policy compliant with the EU Data Protection Directive?

Chart 5

Is your organization registered with the relevant data protection authorities?

Chart 6

Does your organization have a Data Protection and Privacy compliance program?

Source: JEM Consulting, 2017

Chart 7

Do you have a compliance program covering client confidentiality and data protection?

Chart 8

Does a comprehensive inventory exist that details all information, assets, software assets, hardware assets and services?

Chart 9

Does a formal process exist for reporting and handling security incidents, weaknesses, and software issues?

Chart 10

Does your organization have clearly defined responsibilities for managing security incidents?

Chart 11

Does a formal business continuity plan exist?

Chart 12

Do you have a training program for your employees to educate them regarding security, privacy and data protection policies and risk mitigation?

If yes, is the training mandatory?

Source: JEM Consulting, 2017

Social Media Risk

Given the ever-expanding list of social media platforms and efforts made by companies to encourage customers and employees to advocate on these networks on behalf of corporate brands, and the corresponding increase in the number of social media hacks over the past by year—150 percent increase in social media phishing—it's surprising and concerning that only 29.6 percent of respondents consider risks associated with social media to be among their biggest challenges. This points to a lack of understanding in the significance of the new types of digital and social media risks and how to effectively mitigate and manage them.

Employee use of social media

However, companies are not ignoring the risks of social media altogether. In fact, they appear to be paying more attention in the context of employee use of social media. The risks associated with employee use of social media can come in a variety of forms, but companies currently see the most prevalent risk as being the effect on branding and reputation—64.9 percent of respondents mentioned "brand reputation" as a concern about employee use of social media, with the security of employees' social channels, as scams and phishing attacks, as well as fraud and counterfeiting using fake social media accounts become more prevalent, garnering the next highest percentage of respondents at 50.5 percent.

Table 2
Which risks most concern you about employee social media use?

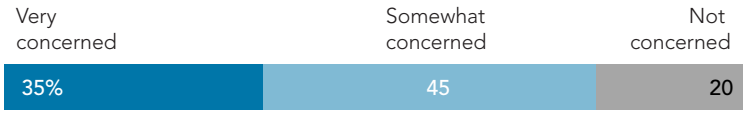
Risk areas	Percent
Brand reputation	64.9%
Security of your employees' social media channels	50.5
Integrations with other systems (e.g., CRM or intranet)	47.5
FTC regulatory compliance	39.6
HIPAA compliance	5.0

Source: JEM Consulting, 2017

Effects on brand reputation One of the primary ways that brand reputation can suffer from employees being active on social media is through staff mistakenly sharing confidential, regulated, or embarrassing information via their social media activity. Eighty percent of companies said they were at least "somewhat concerned" about this sharing of information. It should be noted that this number is much lower for managers of employee advocacy programs, less than 10 percent of whom list inappropriate use of social media by employees as among their top challenges.[5] This again shows a disconnect between professionals managing social media programs, and those primarily charged with managing risk.

Chart 13

Are you concerned about employees mistakenly sharing confidential, regulated, or embarrassing information via their social media activity?



Source: JEM Consulting, 2017

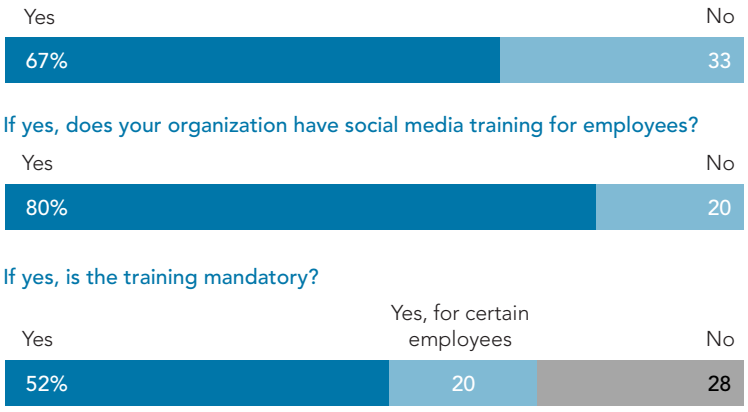
To counter concerns, 67 percent of organizations say they have a social media policy in place and 80 percent of those companies say they have training for employees on social media use, with over half the respondents (52 percent) making that training mandatory for all employees.

Such guardrails are a recommended practice by one top corporate legal officer, but so too is investing in accountability. In *Socially Minded: Convincing the C-suite of Social Media's Benefits*, Eric Dale, chief legal officer of Nielsen, says: "We have a social media policy, as well as internal vetting practices… But the most important thing is that we have a strong corporate culture that is taken seriously and which is reflected in the way people use social media. The culture is not command and control—we call it an 'edge culture,' which means decisions are made at the edge of the organization. We invest in accountability in our employees and they recognize that."[6]

In *Corporate Communications Practices: 2016 Edition*, The Conference Board found that many companies use a similar philosophy of personal accountability as outlined by Eric Dale. According to the report, 72.7 percent of manufacturing companies and 76.9 percent of nonfinancial services companies include in their social media policies prescriptions that employees using social media must "use common sense and reflect on the implications of their statements about the company, its employees or its products and services."[7]

Chart 14

Does your organization have a social media policy?



Source: JEM Consulting, 2017

Targeting employee accounts Although fewer companies showed concern about the security of employees' social channels than they did about hits to brand reputation through employee use of social media, there is still significant concern about hackers and trolls targeting employee accounts and about employees becoming the victim of scams and phishing. More than 80 percent of companies said they were at least somewhat concerned about hackers and trolls targeting employees' social media accounts and a similar percentage were worried about scams and phishing

Chart 15

Are you concerned about hackers and trolls targeting employees' social media accounts?

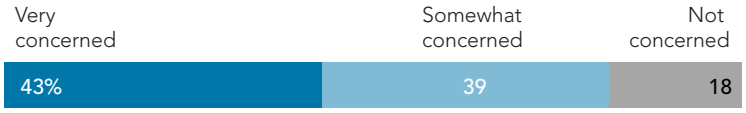


Chart 16

Are you concerned about social media scams and phishing?

Source: JEM Consulting, 2017

Responsibility for Managing Risks

Most companies do not have a fully optimized, managed, and resourced process and program for managing digital and social media risks. Fewer than 10 percent of organizations rated their digital and social media risk management maturity level as "optimized." At the other end of the spectrum, around the same percentage of companies said they were in the initial stage of developing a comprehensive program as those that said their program was "managed," suggesting that there is still a long way to go for many companies to reach a premium state of digital security.

Table 3

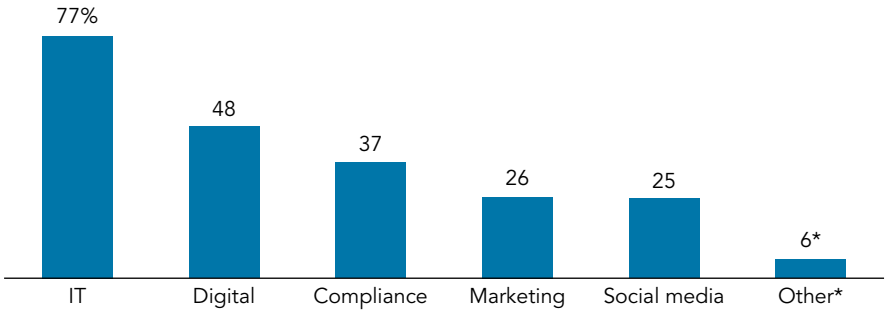
How would you rate your organization's maturity level as it relates to digital and social media risk management?

Risk areas	Percent
Initial Stage (developing a comprehensive program, but managed through individual efforts)	31.2%
Defined (process is defined and confirmed as a standard business process)	26.2
Managed (managed in accordance with agreed-upon metrics)	33.2
Optimized (fully managed, resourced and includes continuous process improvement)	9.4

Source: JEM Consulting, 2017

Chart 17

Which departments/functions are primarily responsible for managing data risk in your organization?



* Other includes HR, Privacy/Protection, Legal, Knowledge Management, Data

Source: JEM Consulting, 2017

As the number and types of digital risks expand, responsibility for managing them is starting to extend beyond the IT department, although in three-quarters of cases the IT team remains the responsible function. Interestingly, around 25 percent of companies responded that either the social media or marketing function were responsible for managing digital or social media risk.

These percentages are significant enough to suggest that these communications-focused departments are expanding their responsibilities as digital-oriented strategies become more popular. At the same time, the growth of digital transformation throughout the organization has resulted in the need for a more formal governance structure that manages digital and social media strategy across functions, rather than a misaligned approach that prevents companies from maximizing the benefits of digital transformation. Seventy percent of respondents stated that they have a digital governance team and/or a Digital Center of Excellence.

These teams and centers need to ensure that they're closely aligned with the IT department or whichever function is responsible for managing digital and social media risk, because sources of risk will grow with the expanded use of digital and social media technologies.

Chart 18

Does your organization have a digital governance team and/or Digital Center of Excellence?

Source: JEM Consulting, 2017

The growing number of cybersecurity risks and the expansion of responsibility for managing these risks beyond the IT department, make it imperative that organizations update their security policies and processes for the digital age. Companies need to review their policies and procedures to ensure they cover these new risks, including third-party, public and consumerized infrastructure, and internal and external threats, such as:

- Bots
- Brand fraud from fake social media accounts
- Brand reputation from employee posts on social media
- Breaches
- Cloud-based applications
- Data collection, storage and management
- Denial of service (DoS) attacks
- Digital trolls
- Email
- Hackers and trolls targeting employee social media accounts
- Malware
- Mobile apps
- Phishing
- Regulatory compliance (ex. HIPAA & FTC)
- Social media scams
- System integration
- Website security

Use of tools and vendors

Often, the most sophisticated defense against new risks come from innovative startups who are constantly assessing threats, rather than those that are developed in house. These tools don't negate the need for in-house procedures to ensure they are up to date (as mentioned on page 2, the Equifax breach was caused by the company not updating its Apache Struts software), but when implemented and managed properly, they can significantly increase digital security.

Chart 19

Do you use tools or vendors to manage your digital risk?

Chart 20

Do you use tools or vendors to help mitigate social media brand, security and compliance risks?

Source: JEM Consulting, 2017

Half of companies use these tools or vendors to ensure their risk mitigation is strong. However, when it comes to social media risks, the percentage is much lower at 33 percent. This suggests that companies are less equipped to handle new risks from social media, which is concerning given the growing use of it at organizations and by employees.

Recommendations

Organizations need to adopt a more comprehensive approach to risk management to address new threats coming from digital, social media and mobile. This can be accomplished through more effective collaboration between the growing number of departments and functions responsible for risk management, including not only IT, but also the digital and social media teams, compliance, marketing and others.

These teams need to work together to update their risk management strategy and governance, ensuring the following:

- A comprehensive approach to risk management, including strategy, governance and enablement through a Digital Center of Excellence. Ensure cross-functional leadership of the DCOE, which acts as a trusted strategic partner to help teams understand and embed new digital and social media technologies and programs safely and effectively. The DCOE provides digital leadership, oversight, training, best-in-class advice, communicate best practices
- Deploy new tools and technologies to proactively identify and manage advanced attacks delivered via email, social media and mobile apps. Keep these tools and technologies regularly updated
- Develop and mandate employee training and enablement to understand and manage these risks
- Formalize policies, processes and programs to address all areas of digital and social media risk
- More comprehensive and effective communication and collaboration between the growing number of departments and functions responsible for risk management

Conclusion

Enterprises have very clearly recognized the need to protect and mitigate risk across their owned infrastructure; however, social media and mobile communications have increasingly expanded that scope to include third-party, public and consumerized infrastructure. Digital and social media channels have accelerated the potential impact of a data breach, which requires organizations to deploy sophisticated remediation measures as quickly as possible.

The recent Equifax hack has shown very publicly how important it is to properly manage digital risk. The fallout of not doing so affects customers and private citizens, but also the overall existence of organizations that fail to mitigate risks.

Endnotes

1 Jackie Wattles and Selena Larson, "How the Equifax Data Breach Happened: What We Now Know," *CNN Tech*, September 16, 2017 (http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html).

2 Lily Hay Newman, "Equifax Officially Has No Excuse," *Wired*, September 14, 2017 (https://www.wired.com/story/equifax-breach-no-excuse/).

3 Michelle Fox, "Equifax Will Not Survive Fallout from Massive Breach, says Technology Attorney," CNBC, September 14, 2017 (https://www.cnbc.com/2017/09/14/equifax-will-not-survive-fallout-from-massive-breach-says-technology-attorney.html).

4 Fox, "Equifax Will Not Survive Fallout from Massive Breach, says Technology Attorney;" Berkeley Lovelace Jr., "Cramer: 'Equifax CEO Should be Fired Today' After Data Breach Fallout," CNBC, September 14, 2017 (https://www.cnbc.com/2017/09/14/cramer-equifax-ceo-should-be-fired-today-after-data-breach-fallout.html); John Bowden and Ali Breland, "Two Equifax Executives Resign In Wake of Massive Data Breach," *The Hill*, September 15, 2017 (http://thehill.com/policy/cybersecurity/350951-two-equifax-executives-resign-in-wake-of-massive-data-breach) ; Kevin McCoy, "Do You Want to Sue Equifax Over the Cyberbreach? Winning a Lawsuit May Not Be So Easy," *USA Today*, September 22, 2017, (https://www.usatoday.com/story/money/2017/09/22/do-you-want-sue-equifax-over-cyberbreach-winning-lawsuit-may-not-so-easy/684455001/).

5 Jen McClure, *State of Employee Advocacy: 2017 Edition*, JEM Consulting and Advisory Services, (forthcoming).

6 Alex Parkinson, *Socially Minded: Convincing the C-suite of Social Media's Benefits*, The Conference Board R-1629-17, 2017.

7 Matteo Tonello and Alex Parkinson, *Corporate Communications Practices: 2016 Edition*, The Conference Board R-1600-16-RR, 2016.

Methodology

The 2017 State of Digital and Social Media Risk Management was conducted by JEM Consulting & Advisory Services, a Silicon Valley-based management consultancy. The study highlights trends and best practices for digital and social media risk management, and provides a useful resource for teams responsible for managing the growing number and types of digital and social media risks in their organizations. The online survey-based study was conducted in Q1 2017. More than 200 responses (202) were gathered from leaders with responsibility for digital governance and/or digital risk management. The sample included 90 percent US-based organizations of all sizes from small-medium businesses to large enterprise organizations in all sectors, including primarily public and private companies, but also governmental and educational institutions, and nonprofits. More than 50 industries were represented in the sample, including both B2B and B2C companies.

About the Authors

Jen McClure is CEO of JEM Consulting, a Silicon Valley-based management consultancy for the digital age. She is one of the original authorities on digital and social media. More than a decade ago, she anticipated the significant impact that these technologies would have on business, media, culture and society. This led her to cofound the Society for New Communications Research (SNCR) in 2005, a think tank focused on these technologies, which merged with The Conference Board in 2016. She now serves as a program director for The Conference Board and advisory board chair for SNCR. Prior to founding JEM, McClure was VP of digital and social media at Thomson Reuters, where she founded the company's Digital Center of Excellence and oversaw digital strategy, enablement and governance. McClure received her Bachelor's degree from Sarah Lawrence College, and her Master's degree from Stanford University.

Alex Parkinson is a senior researcher, corporate philanthropy, and associate director, Society for New Communications Research of The Conference Board (SNCR). He led the integration effort between SNCR and The Conference Board when the two organizations came together in February 2016 and now serves on the combined entity's advisory board. He is the executive editor of *SNCR 2020: Exploring New Communications Tools and Technologies*, the *Giving Thoughts* blog and online publication series, and *Framing Social Impact Measurement*, a compendium report that responds to the growing demand for information on evaluating the performance of grants. He is the author of *Socially Minded: Convincing the C-Suite of Social Media's Benefits*, *Unlocking the Value of Integrated Corporate Communications and Marketing*, *Making Sense of Social Impact Bonds for Companies and Better Together: Why A United Front Can Propel Diversity and Inclusion and Corporate Philanthropy in the United States*, and co-author of *Corporate Communications Practices: 2016 Edition*.

ABOUT THE *SNCR 2020 SERIES*

The *SNCR 2020 Series: Exploring New Communications Tools and Technologies* is an online publication from the Society for New Communications Research of The Conference Board (SNCR), which addresses emerging topics in new and emerging communications tools and technologies, including digital, social media, and mobile, and their effect on business, media, health, law, culture, and society. Subscribe for free to the SNCR blog and the *SNCR 2020 Series* at www.conferenceboard.org/sncrblog.

ABOUT THE SERIES DIRECTOR

Matteo Tonello is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, shareholder activism, corporate sustainability, and philanthropy. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors, and professional firms. He is the author of several publications, including *The Corporate Governance Handbook: Legal Standards and Board Practices*, *Sustainability in the Boardroom*, *Institutional Investment*, and the annual *US Directors' Compensation and Board Practices* report. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets and the Advisory Council to the Sustainability Accounting Standards Board (SASB). Prior to joining The Conference Board, he practiced corporate law at Davis Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

ABOUT THE SOCIETY FOR NEW COMMUNICATIONS RESEARCH OF THE CONFERENCE BOARD

The Society for New Communications Research of The Conference Board (SNCR) is dedicated to the advanced study of the latest developments in new and emerging communications tools and technologies, including digital, social media, and mobile, and their effect on business, media, health, law, culture, and society. SNCR's Fellows include a leading group of futurists, scholars, business and communications leaders, members of the media and technologists from around the globe—all collaborating together on research initiatives, educational offerings, and the establishment of standards and best practices. Established as an independent not-for-profit institution in 2005, SNCR joined The Conference Board in 2015 to operate as part of its larger organization. Visit www.conferenceboard.org/sncr for more information.

THE CONFERENCE BOARD is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance *and* better serve society. The Conference Board is a non-advocacy, not-for-profit entity, holding 501(c)(3) tax-exempt status in the USA.

THE CONFERENCE BOARD, INC. | www.conferenceboard.org

AMERICAS
+1 212 759 0900 | customer.service@conferenceboard.org

ASIA
+65 6325 3121 | service.ap@conferenceboard.org

EUROPE, MIDDLE EAST, AFRICA
+32 2 675 54 05 | brussels@conferenceboard.org

THE COMMITTEE FOR ECONOMIC DEVELOPMENT OF THE CONFERENCE BOARD
+1 202 469 7286 | www.ced.org

THE DEMAND INSTITUTE
A Division of THE CONFERENCE BOARD
+1 212 759 0900

THE CONFERENCE BOARD OF CANADA | +1 613 526 3280 | www.conferenceboard.ca