Cyber Risk Correlations in the GRAFT Framework

AUTHOR:
Lois Tullo, Executive-in-Residence, Global Risk Institute

Strategic Implications of Cyber & Data Risk, and Cyber Dependency

TOP RISK CORRELATION SERIES 2018

This article is the first in a series that will focus on applying risk correlations to further a robust approach to the management of emerging risks. The paper applies the correlation matrix from the Global Risks and Trends Framework (GRAFT)[1] to a specific topic in order to highlight risk interdependencies, and to assist in the analysis of strategic implications. The correlation matrix aims to provide both strategic insights and recommendations for an organization and is based on the premise that risk events do not happen in isolation - events are not typically the result of one risk or trend, but rather a combination of risks and/or trends. It is through the lens of inter-relationships that we examine the top risks and trends for 2018.

We look at the highest ranked risks and trends, and their correlation and combination with other risks and trends, to identify the strategic implications for organizations within the financial services sector. From our research[2] we have identified 5 key risks and trends correlations, informed by many of the risk ranking surveys that are summarised in the appendix.[3]

TOP RISK RANKING CORRELATIONS

The 5 top risk and trend correlations and combinations for 2018 are:

1. ***Cyber Attacks/Data Fraud or Theft/ Cyber Dependency,[4]***
2. ***Climate Change/Extreme Weather Events/Natural Disasters,***
3. ***Interstate Conflict/Increasing National Sentiments/Regulatory Change,***
4. ***Income and Wealth Disparity/Debt Levels/Asset Bubble, and***
5. ***Large Scale Migration/Failure of Global and National Governance***

This series on the top 2018 risk correlations is also informed by numerous risk events of 2017. Consistent with GRI's annual survey of Chief Risk Officers, and unsurprisingly, cyber security and data attacks tops the list. Business interruption risk events in 2017 have become more frequent and continue to accelerate in 2018. It is useful to look back on some of the most significant recent events for insight into the future. As for many of the top risks/trends and their correlations, the dialogue is changing from "if" to "when". Prevention along with stress tested response preparation has become the new norm in considering and in addressing cyber and data risks. This paper aims to highlight the strategic implications for organizations in the financial services industry.

1 *GRAFT is a robust, systematic process for identifying, assessing, and responding to strategic risks posed by Global Risks and Trends; it facilitates identification of potential opportunities to leverage them for the organization's benefit.*

2 *See Appendix for 2018 Risk Ranking Summaries.*

3 *The appendix supports step 3 and 4 of the GRAFT process. Reviewing the Risks Ratings will help organizations to understand global risks and trends, and to aid in ranking and prioritizing of risks and trends.*

4 *Rise of cyber dependency due to increasing digital interconnection of people, things and organizations.*

Cyber Attacks/Data Fraud and Theft/ Cyber Dependency

In the years 2017/18 we have witnessed rising number[5] and cost[6] of cyber attacks and data theft.

Figure 1: Number of Data and Cyber Attacks 2005 - 2017

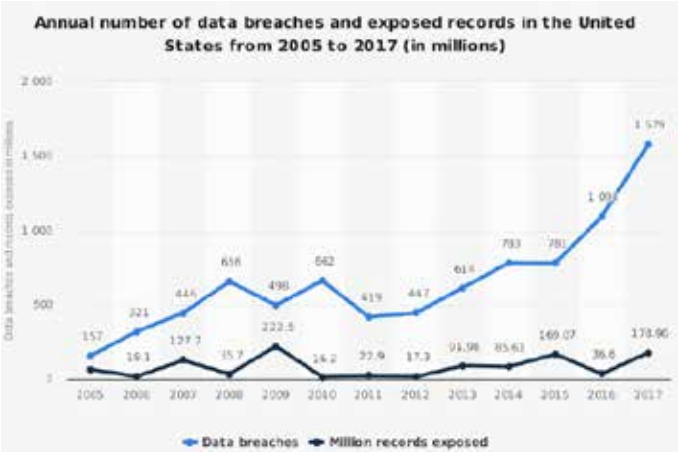
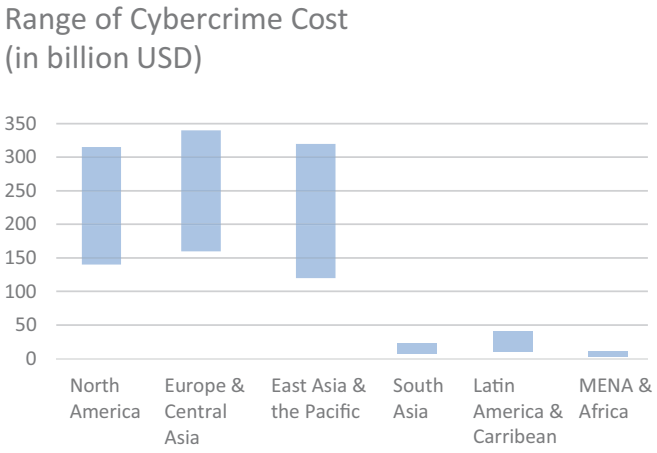


Figure 2: Cost of Cyber Attacks 2017



A few of the largest examples include:

- ***143 million US citizens had their social security numbers and addresses stolen from consumer credit rating agency Equifax, exposing them to the risk of identity theft.[7]***
- ***The Wannacry attack, a strain of ransomware, hit hundreds of thousands of companies including public utilities, hospitals and large corporations. The attack was centred in the Ukraine, but spread quickly across 150 countries.***
- ***Data of 87 million Facebook users was improperly used by Cambridge Analytics with political influence linked to the data sharing.***
- ***A cyber security researcher has claimed that Narendra Modi's NaMo app is at the centre of a dispute on data privacy with data being sent to third party, a US based analytics company called CleverTap.[8]***

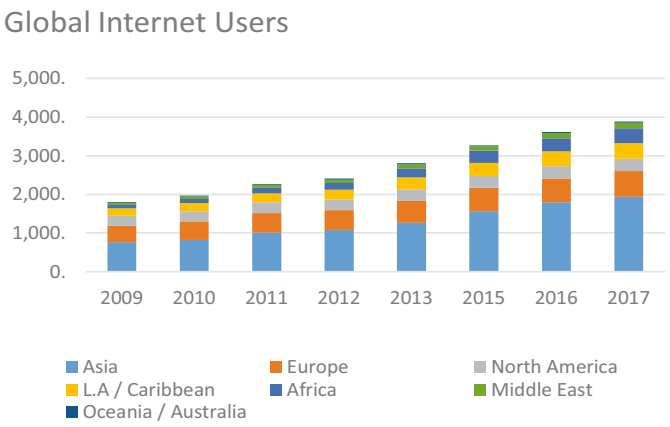
5 *Statista, "Cyber crime: number of breaches and records exposed 2005-2017", (2018)*

6 *James Lewis, "Economic Impact of Cybercrime – No Slowing Down", McAfee, pg.3, (Feb 2018).*

7 *Chartis, "Big Bets - Cyber Risk Quantification and Analytics", (Feb 13, 2018).*

8 *Amy Kazmin, "Narendra Modi's personal app sparks India data privacy row" Financial Times, (Mar 28, 2018).*

Figure 3: Global Number of Internet Users 2009 - 2017



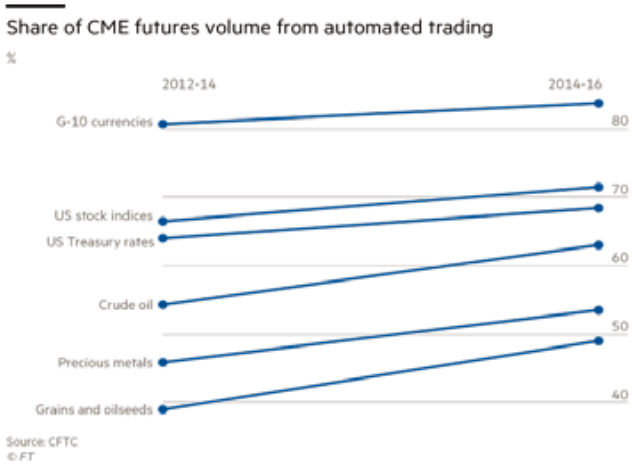
At the same time, cyber dependence is rising.

Internet usage[9] has risen in 2018 to over 50% of the population, with 95% usage in North America and 85% in Europe. While usage is just 48% in Asia, that translates to over 2B users, or almost half of world usage.[10]

Research indicates that increasing **cyber dependence** is evidenced in smartphone addiction and adverse unintended consequences such as impaired attention, reduced numerical processing capacity, and changes in social cognition.[11]

Financial markets are also experiencing increased cyber dependence as can be seen in the increase of automated trading across all markets[12] and the rising marketshare of equity ETFs to 60% of trading and AUM of $4.4T US.[13]

Figure 4: Automated Trading Volume



9 *Statista, "Number of worldwide internet users 2009-2017, by region",(2018).*

10 *Miniwatts Marketing Group, "Internet Users in the World by Regions – December 21, 2017" (2018).*

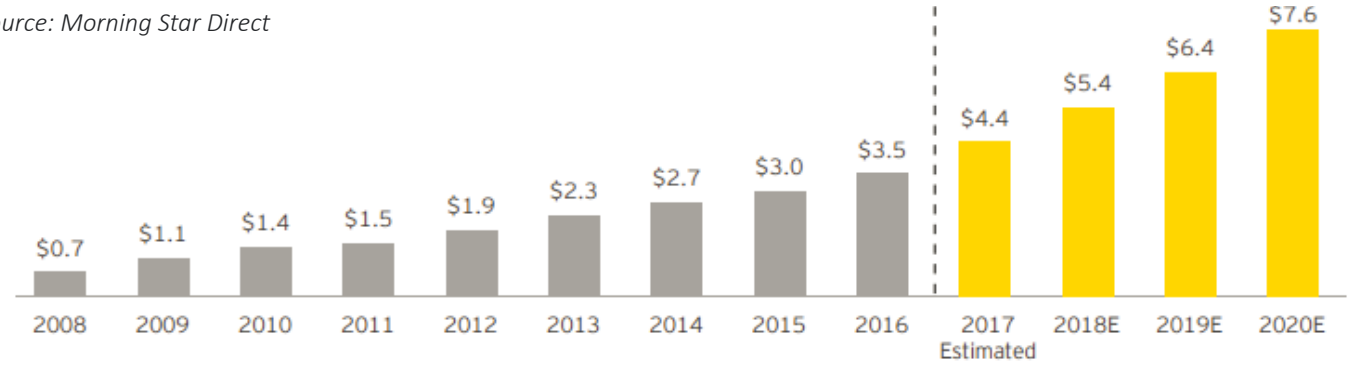
11 *Aviad Hadar et al., "Answering the missed call: Initial exploration of cognitive and electrophysiological changes associated with smartphone use and abuse", PLOS, (Jul 5, 2017).*

12 *Gregory Meyer, Nicole Bullock, and Joe Rennison, "How high-frequency trading hit a speed bump", Financial Times, (Jan 1, 2018).*

13 *Ernst & Young, "Reshaping around the investor – Global ETF Research 2017", pg 4, (2017).*

Figure 5: Global ETF AUM

Source: Morning Star Direct



The correlation and combination of risks and trends leads to an increasing impact of risk events. We outline We outline below (Fig. 6) some of the interactions between, and resulting from, data and cyber attacks of 2017/18 and growing cyber dependence.

The correlation mapping of risks and trends shows the interaction of risks (rectangles) and trends (ovals) and is color-coded by risk cluster (Purple – Technological, Red – Societal, Blue – Economical, Green – Environmental, and Orange – Geopolitical).

The GRAFT correlation matrix facilitates an examination of the knock-on effects of risk events and trends. For example, the accessing of US pre-election emails can be tied in as one of the justifications for the US sanctions on Russia, and election rigging can be tied to the increasing ideological divisions within society, which is also affected by the growing income and wealth disparity. We also saw examples of failure of critical infrastructure in Atlantic city's services were shutdown caused by the SamSam crew ransomeware attack. Origin of the crew is at this time unknown.[14]

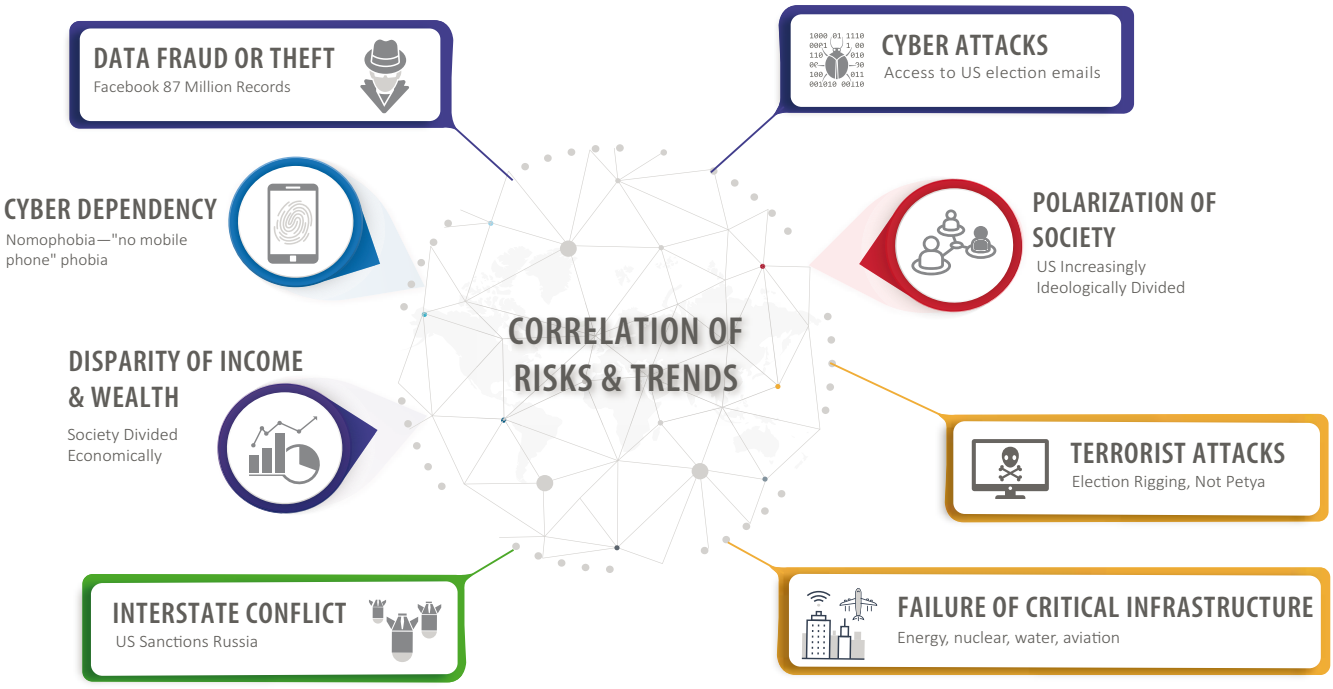
By looking at the events of 2017 using the GRAFT correlation matrix we can learn from the past and use those learnings to look forward and consider how risks/ trends may evolve.

Strategic Implications for Financial Institutions

For financial institutions, the strategic implications of the increasing cyber / data attacks, amplified by rising cyber dependency, are particularly acute. That said, they are increasing their own reliance on technology for their

14 *Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder", The New York Times, (Mar 27, 2018).*

Figure 6: Data, Cyber Attack and Dependency Event Risk Correlation Mapping 2017



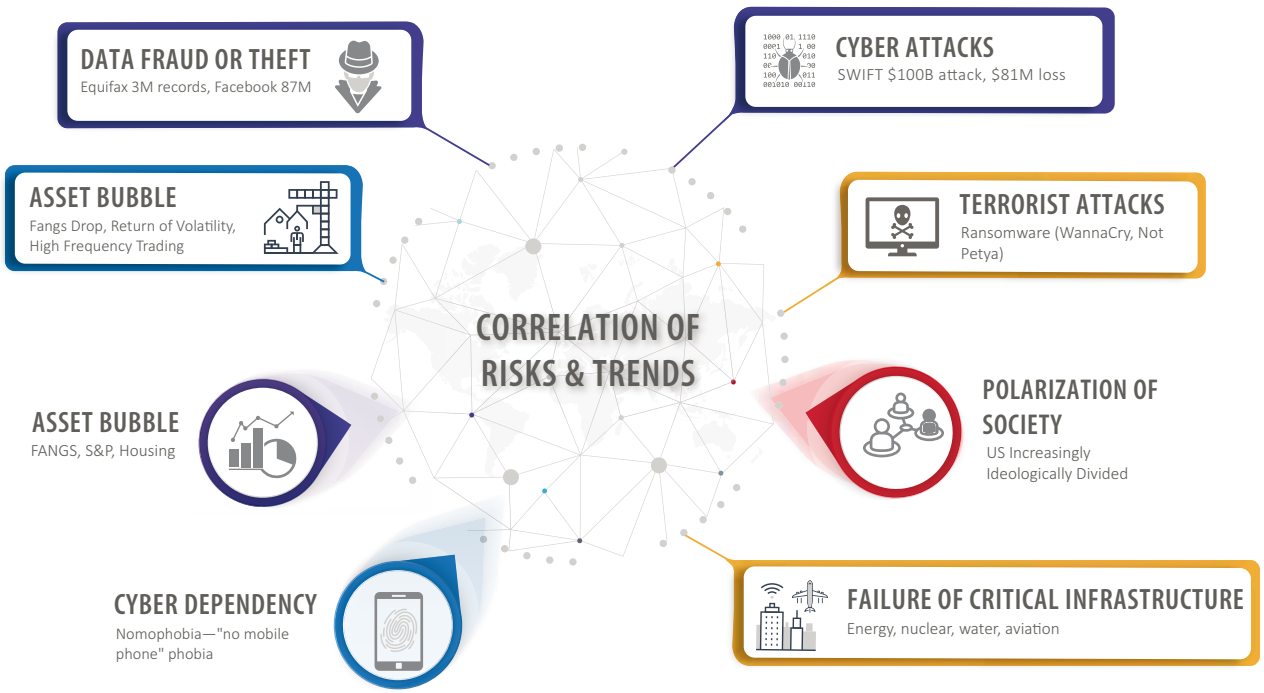
businesses which increases their potential risk exposure. Consider for example the growing array of product and service offerings that are technology based, and the growing opportunities for use of data, along with platforms such as high frequency trading, but also the growth in telecommuting/work from home, BYOD (bring your own device), and Open API trends . Cyber safety is becoming more challenging. Preparing and testing of backup plans, including business disruption resulting from cyber incidents, are critically important, not just to the ongoing provision of service, but also for preserving trust.

The risk implications for financial institutions span from idiosyncratic effects (e.g., cyber security incidents at a particular institution) to financial system safety (e.g., cyber attacks affecting the broader financial system, or critical infrastructure breakdowns) and overall financial system stability.

The interrelationship of cyber dependency/cyber attacks/ data theft & fraud affect asset managers as for both the firms and industries, there is increased opportunity as well as vulnerability. For example, asset returns, particularly for tech-based stocks, can be affected by positive as well as negative events relating to data management capabilities, with higher stock market volatility. Default rates may be affected by stock market volatility, as well as asset bubble corrections. Societal impacts associated with growing wealth and income disparity and polarization of society, as well as changes to the labour market associated with technology, may also lead to higher default rates. The future of high frequency trading, on-line trading and banking are vulnerable to rising cyber safety concerns. Blockchain and cryptocurrencies are also emerging, fueled by a rising trend for disintermediation which in turn reflect changing societal influences.

Recent cyber incidents and existing cyber trends are the foundation for looking into the future and form the basis of identification and consideration regarding the potential strategic implications of the risk and trend correlations. Figure 7 provides an example based on risk events and trends affecting the financial industry.

Figure 7: Data, Cyber Attack and Dependency Event Risk Correlation Mapping for Financial Services



Key Insights: Based upon the Impact of Movement in the Global Risks and Trends

The correlation matrix (Table 1 below) is a tool for organizations to identify key insights stemming from the correlation of the examined global risks and trends. Organization's management compare the correlation relationships to the organization's mission statement (what is our purpose) and objectives (what are we trying to achieve). The exercise of comparing the GRAFT relationships to the mission and objectives facilitates a discussion confirming and potentially contradicting participants' preexisting views. Organizational leaders confront the growing array of factors, both domestic and international, that could potentially result in cyber and data attacks. They may conclude that certain areas of their business (e.g., customer data), would be more at risk than others. The exercise may lead to potential identification and segmentation of critical system, applications, and data from potential cyber breaches.

Table 1: Correlation Matrix- Financial Services Industry Implication and Key Insights

Primary risk or trend	Correlated risk or trend	Magnitude[15] of correlation and implication	KEY INSIGHTS - Events or potential events stemming from correlation of trends & risks
Cyber Attacks	*Cyber Attacks*	*The number[16] , size, scope, and impact of cyber attacks is increasing, as demonstrated by recent ransomware attacks, for example WannaCry and Not Petya, and attacks affecting customers data . The issue is not solely financial services issues, affecting many technology-dependent companies such as Facebook and Equifax, as well as a variety of retailers including Target, Home Depot and Saks.*	*New/Expanding digital strategies increase vulnerability to cyber attacks at the same time as cyber attacks are become more frequent and sophisticated. Costs of cyber crime are rising. Cyber breaches can erode trust.* ***Cyber security is therefore critically important and must be at the forefront when considering digital strategies.*** *Mindset must change from "if" to "when" a cyber breach will occur, necessitating* ***development and testing of response plans for various scenarios that include communication strategies*** *for all key stakeholder groups aimed at preserving trust.* *More organizations are creating a partnership of the Chief Information Officer CIO and of the* ***Chief Information Security Officer*** *(CISO). With a view to strategy, the CIO's charter is to ensure information is available to run the business; the CISO's charter is to ensure security without affecting availability of business services,[17] as well as preparing the organization for when a cyber attack is successful.*

15 *Magnitude based upon serverity and likelihood is risk event.*

16 *See Figure 1 and 2*

17 *Grant Bourzikas, "Changing Role of the CISO", CISOMAG, (Jan 4, 2018).*

Cyber Attacks	*Cyber Attacks*	*cont'*	*Establish and practice legal involvement (internal or external) to ensure **duty of confidentiality and solicitor-client privilege** in any cyber investigation.* *Technology risks require **heightened level of understanding and oversight** by audit functions and by boards of directors. **Live Cybergames** should include the board, be directed by the CISO and involve other C-suite management. The board should have the requisite technology expertise to contribute.*
Cyber Attacks	*Data Fraud or Theft*	*Organizations are at risk of losing customer trust if their private information becomes publicly available, is misused or corrupted.* *The attacks on SWIFT are notable for two things:* • *the attacks were against the banking system itself, not customers; and* • *the attackers targetted **modifying**, not stealing, **information**.* *Perpetrated through phishing, malware allowed attackers to delete outgoing financial transfer requests and amend those received. The attackers also had the ability to amend customer accounts and even intercept and change PDF statements to successfully cover their tracks.[18]* *Data "landmines" can mislead decision making across organizations, governments, and individuals, especially if data analytics cannot confirm the validity of the source data.*	*Outline the organization's alignment with industries "**Sheltered Harbor**"[19] initiative.* *Data protection strategy and initiatives rollout to address potential **integrity issues or "weaponization" of data**. The implications of which are shutting down all operations as the integrity of "End of Day" numbers which pose the reputational risk degradation.* *Review data collection and use practices for employee and consumer personal data. **Enhance privacy policies** and data compliance programs, as well as audit coverage. Address issues raised in audit and government compliance reviews.* *Consider using third party services to assess security posture, configure privacy and security policies and incident response plans.*
Cyber Attacks	*Rise of Cyber Dependency*	*Vulnerability to cyber attacks is increasing because of cyber dependency.* *Over 3.5 billion passwords are available on the darkweb, of which the latest find was 1.4 billion passwords in plaintext available for sale which were valid, indexed, and updated found December, 2017, by 4iQ.[20]*	*Provide frequent **employee training** on the importance of cyber security, expected cyber "hygiene" practices, and common as well as new threats. Employ phishing tests.* *Introduce and enforce **BYOD and mobile computing policies**.* *Establish **multifactor authentication** protocol.*

18 Kevin Murphy, "Security Think Tank: Data integrity breaches – the challenge facing banks", Computer Weekly, (Feb 2018).

19 A sheltered harbor strategy combines proactive, secure data storage with a quick, cooperative recovery plan to get your organization through a major catastrophic event faster than on your own. By storing your organizations's data in Sheltered Harbor's industry-standard format, a peer organization or processor can restore account information and keep your business up and running limiting potential service interruption.

20 Julio Casal, "1.4 Billion Clear Text Credentials Discovered in a Single Database", Medium, (Dec 8, 2017).

Cyber Attacks	*Rise of Cyber Dependency*	*Use of personal devices at work increases potential vulnerability for companies due to indirect control of device security and activity.* *The BYOD market is on target to reach nearly $367 billion by 2022, up from just $30 billion in 2014.*[21] *59% of organizations allow employees to use their own devices for work purposes, (downloading apps). Another 13% had planned to allow use within a year.*[22] *87% of companies rely on their employees using personal devices to access business apps.*[23]	*Consider running the organization's software in a secure,* **isolated sandbox** *on the phone, or using* ***device integrity scanning applications****.*[24] *Consider implementing* **white-listing** *to prohibit installation of all unapproved applications, or implementing a secure sandbox that isolates the organization's data and applications from all other data and applications on the mobile device.*
Cyber Attacks	*Interstate Conflict*	*Aggressive shift of international cyber climate, both in attacks and international cyber policies. Attribution of Nation state attackers, such as NotPetya to Russia (their first priority is collecting military and diplomatic information), and China's Group 61398, who are implicated in stealing trade secrets from companies such as Westinghouse and US Steel (is to enable their State Owned Enterprises (SOEs) to compete and dominate on a global economic level).*[25] *Recent sanctions have been linked partially to cyber attacks.*	*State-sponsored hackers can hide attacks in encrypted SSL*[26] *traffic to evade detection. As a result, network security solutions, such as next-gen firewalls and intrusion prevention systems, need to be able to* ***inspect all incoming and outgoing traffic for threats*** *-- not just the data that is sent in plain text.* *Increased level of traffic monitoring is required to protect against sophisticated nation state attacks. Protect web application data with a* ***Web application firewall*** *(WAF), which filters all application access by inspecting both the traffic toward the application and the response traffic from the application. A WAF offers granular control of the application's data flow and is capable of protecting against various attacks including SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks, among others.*[27]

21 Anna Johansson, "Growth of BYOD proves it's no longer an optional strategy", Betanews, (2017).

22 Teena Maddox, "BYOD, IoT and wearables thriving in the enterprise", TechPro Research, (Jan 4, 2016).

23 Information Solutions Group, "Syntonic 2016 Employer Report: BYOD Usage in the Enterprise", Syntonic, pg 9, (2016).

24 Jessica Keyes, "BYOD: Mobile Devices Threats and Vulnerabilities", IT Performance Improvement.

25 Leo Taddeo, "Nation-state cyber attacks come out of the shadows", NewStatesman Tech, (Apr 12, 2017).

26 SSL provides a secure channel between two machines or devices operating over the internet or an internal network. This turns a website's address from HTTP to HTTPS, the 'S' standing for 'secure'. HTTP is unsecure due to data being transferred in plain text.

27 Kasey Cross, "5 Ways to Fight Nation-State Attacks", eSecurity Planet, (Dec 21, 2015).

Cyber Attacks	*Interstate Conflict*	*Rise in Tier II & III Cyber nations such as North Korea, Iran, Vietnam, and Ethiopia. Increases in their capacity, readily availability of tools developed by Tier I nations, and the leak of NSA tools.*[28]	***Increase cooperation with federal law enforcement** to identify the use of foreign language in its malware code; malware compile times corresponded with business hours of a countries major cities; data stolen is intellectual property useful mainly to foreign governments.* *Coordinate efforts with the **Canadian Centre for Cyber Security** and the **National Cyber Crime Coordination Unit** being newly established for the end of 2018.*
Rising Cyber Dependency	*Illicit Trade*	*The rising use of personal devices and the influx of social media has increased the available access points for criminal and employees to hide illegal transactions, resulting in direct losses and increased regulatory AML fines.* *Ransomware now represents 40% of all malware attacks. Global ransomware damage costs predicted to exceed $5 billion in 2017.*[29] *91% of cyberattacks begin with spear phishing email, which are commonly used to infect organizations with ransomware.*[30] *The Deep/Dark Web (which is not indexed or accessible by search engines) may be as much as 5,000 times larger than the surface web, and growing at a rate that defies quantification, according to one report.*	*Better prevention and detection of illegal activities are required to protect the company against direct losses as well as associated fines and reputational damage. Consider potential for enhancements including use of **AI's behavioral analytics capabilities to prioritizes investigation queues for Suspicious Activity Reports.***[31] *Investigate options for enhancing security associated with cross-border electronic transactions. Industry examples such as IBM's collaboration with KlickEx Group, and Stellar.org, provide a new electronic currency exchange network to carry out their cross-border payments, security lending, private equity administration, forex payments netting and financial trading using a blockchain platform*[32] *Increase spending and institute employee cyber training that includes **spear phishing attack, and ransomware simulations**.* *Engage third party experts for education as well as assistance in development of a **Deep/Dark Web** strategy, including a monitoring and response plan.*

28 Scott Shane, Nicole Perlroth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core", The New York Times, (Nov 12, 2017).

29 Steve Morgan, "Global Ransomware Damage Costs Predicted To Exceed $5 Billion In 2017" , Cybersecurity Ventures, (May 18, 2017).

30 Steve Morgan, "Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019", Cybersecurity Ventures, (Nov 14, 2017).

31 FICO, "Top 5 Fraud & Security Posts: AI Meets AML (and Hackers)", (8 January, 2018).

32 ACCEO Tender Retail Team, "IBM Blockchain cross-border payments to radicalize existing systems", ACCEO Tender Retail, (Jan 4, 2018).

Rising Cyber Dependency	*Asset Bubble*	*60 per cent of trading — twice the share of 10 years ago — is "passive and quantitative investing." Nearly half is high-frequency trading by algorithms; it's responsible for pretty much all of the stock market's volume gains this century. Algorithms have caused the stock market to decouple from important information streams that existed in a human-dominated market.*[33] *High frequency trading, and trading algorithms increase the inter-dependences between various financial instruments and asset classes. HFT has been linked in the past to flash crashes, with the increase in ETFs and algorithmic trading, there is increased risk of accelerated correction in the market. On October 15 2014, when the 10-year US Treasury bond yield suddenly tumbled and then roared higher again, a 37-basis point intraday move so sharp that in theory it should only be expected once every 1.6bn years.*[34] *Recent fall in Facebook valuation linked to data sharing investigation at from March 16th, 2018 $185, to $153 on March 28th, 2018.*	*Implement **risk correlation to direct stress testing** and back testing of trading algorithms.* *Implement crisis market monitoring and response strategy. New "**crash algorithms**" to be developed to trade during periods of market stresses in order to profit from these periods.*[35] ***Stress test** effects of market illiquidity in relation to accelerated market corrections and flash crash events.* *Organizational **reputational risk and risk appetite** are increasingly influenced by the setting, monitoring and enforcing of **data governance policies.***
Cyber Attacks	*Profound Social Instability*	*Research shows social media increases the bias of individuals by tailoring the information delivered to individuals by their previous search criteria.* *62% of data breaches were linked to identity theft.*[36] *Cyber attacks in regions with developing social instability will exacerbate.*	*Identify potential direct and knock-on effects on the organization's geographic locations as well as the organization overall. Use stress testing/ scenario analysis to assess impact.* *Establish **Early Warning Indicators** to monitor social instability "**hot spots**" and trends in conjunction with locations of cyber attacks. Pro-actively develop risk event responses for deployment as needed.*

33 Leonid Bershidsky, "How stock-market trading is becoming a lot like bitcoin trading", Toronto Star, (Feb 6, 2018).

34 Robin Wigglesworth and Joe Rennison, "Bond trading: technology finally disrupts a $50tn market", Financial Times, (May 9, 2018).

35 Didier Sornette and Susanne von der Becke, "Crashes and High Frequency Trading", Social Science Research Network, (Dec 24, 2011).

36 Gretel Egan, "Scary Data Breach Statistics of 2017", Wombat Security, (Oct 27, 2017).

Cyber Attacks	*Failure of Critical Infrastructure / Information Infrastructure*	*Critical infrastructure and information infrastructure hack, example, the cyber attack on Ukraine's power grid that left 700,000 people without electricity for several hours,[37] and the penetration of safety systems of a petrochemical plant in Saudi Arabia by hackers.[38]* *The attack on Canadian payment service provider TIO Networks (60,000 utility bill payment kiosks), owned by PayPal, exposed the personal and financial information of 1.6 million customers in November of 2017.[39]*	*Develop an infrastructure **external/internal vulnerability scanning** and assessment capability.* *Undertake regular **cyber crisis planning, preparedness and response exercises** with government, military, and industry partners. Including live test contingency backup for dependent infrastructure.* *Develop the **playbook** for who is responsible for what decision making and communication before the crisis happens. Coordinate with industry, government, and vendors who is responsible to restore systems and confidence in the system if required.*
Cyber Attacks/ Cyber Dependence	*Unemployment/ Under-employment*	*Rising unemployment caused by new technology, as well as lack of workers with appropriate skills for new technology environment.* *Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021.[40]*	*Cyber technology skill/HR plan and renewal program.* *Designate a **CISO and Data Protection Officer**.* ***Partner with cyber research and startup hubs** with both the private and university hubs to ensure an agile future resource capability by providing appropriate skills training.*
Cyber Attacks	*Adverse affects of technological advances*	*Update applications to ensure current security best practices - Windows XP is run on nearly one in 10 desktop computers even though Microsoft stopped writing and distributing security updates for it in 2014.[41]* *Technology spending has increased on average by 10 – 15% per year.* *Average time spent on technology is over 7 hours per day. Research shows a lower desire to engage in personal interaction vs gaming or social media.*	***Technology budget and technology debt[42] planning** to address risk of cyber attacks.* ***Harden the legacy systems** by doing a formal risk assessment of a particular system to identify what elements are most at risk, and replacing that part of the system; and, in some industries, replacing the legacy system completely." Systems that are no longer supported with patches should be quarantined from any other system environment, especially endpoint networks.[43]* *Assess technology impact on employees and customers to identify and address both positive and negative implications.*

37 James Titcomb, "Ukrainian blackout blamed on cyber-attack", The Telegraph, (Jan 5, 2016).

38 Clifford Krauss, "Cyberattack Shows Vulnerability of Gas Pipeline Network", The New York Times, (Apr 4, 2018).

39 Lewis, "Economic Impact of Cybercrime", pg 21.

40 Steve Morgan, "Cybersecurity Jobs Report 2018-2021", Cybersecurity Ventures, (May 31, 2017).

41 Angus Batey, "Old technology creates an open door for cyber attackers", Financial Times, (Oct 2, 2016).

42 Techopedia

43 Reto Zeidler, "The Living Dead: How to Protect Legacy Systems", Security Intelligence, (Jul 20, 2017).

Cyber Attacks / Data Fraud & Theft	*Increasing National Sentiment*	*Change in regulatory environment in US & EU (GDPR May 25, 2018) with protectionist policies. Potential change in degree of freedom of movement and security of information increasing risk of losing security and privacy of information.*	***Monitor regulatory changes and proposed changes** in US and world regulation as related to Financial Services. Lobby US government to ensure protection of access to US market.* *Develop, implement, and audit data protection **regulatory compliance strategy** for both cyber and data sharing protection.* *Develop **strategy for regulatory compliance and reporting**:* • *such as how to meet 2hr to 24hr time to recover requirements.*
Cyber Dependency	*Rising Income and Wealth Disparity*	*Cyber dependency is increasingly a barrier to low income individuals having access to increased income and wealth. Access to education to enter into the technology economy is less accessible to low income individuals. Lower level jobs are at greater risk of being illuminated by technology.*	*Sponsorship of low income cyber technology training programs.* *Partner with government and academia to develop training and co-op placement*

The next steps for an organization implementing the GRAFT framework are to consider these strategic implications and key learnings in light of their business strategy, and strategic assumptions. Cyber dependency provides both opportunities and risks, while cyber attacks and data fraud present only downside risk for organizations. The strategic assumption that organizations can rely on the safety, security, and integrity of their systems and data must be constantly questioned, monitored, and tested. With this assumption in question, the business strategies that have take this for granted must be evaluated with this new awareness, and modified or enhanced to ensure that they are attainable.

CONCLUSIONS

The inter-relationship of risks and trends can materially heighten risks, making their identification and corresponding impact assessment all the more important. Giving consideration to the relationships of risks and trends can lead to new insights for enhancing the management of risks. This consideration should help reduce potential downside impacts and may also lead to identification of new opportunities.

The GRAFT process includes a systematic approach to consideration of correlations that supports identification of insights for proactive adaptation of strategies. Business strategy and risk management must now integrate cyber preparedness and resilience in a new way. Plans to address both a worst case coordinated systemic attack, and the daily barrage of one off uncoordinated attacks must be examined on not only a technical view but also from a business-critical approach to strategy.

Specific to cyber threats, as shown in this paper, the combination of rising cyber dependence and the increasing prevalence and sophistication of cyber attacks has heightened vulnerability, requiring organizations to consider cyber resilience in a new way and augment their approach to cyber risk management. Beyond prevention, organizations need to explicitly plan for a coordinated and damaging system penetration, and to test their plan on a regular basis. Inter-organizational, national and international coordination with governments is now critical for ensuring the safety and integrity of critical systems, data and infrastructure.

The correlation of cyber attacks, data theft & fraud, and cyber dependency is the first in GRI's examination of key risk correlations. GRI will be publishing additional papers to examine other key risk and trend correlations identified for 2018 .

APPENDIX:

RISK RANKINGS 2018

1. World Economic Forum
   Top Risks 2018 Report
2. Global Risk Institute
   Summary of Key Risks 2018
3. Eurasia Group
   Top Risks 2018 Report
4. NC-State-Protiviti-Survey
   Executive perspectives on top risks for 2018
5. Allianz
   Allianz Risk Barometer Top Business Risks 2018
6. CEB Risk Management Leadership Council
   Top 10 Emerging Risks Q2 2017
7. Control Risk
   Risk Map- Top 5 Risks
8. Blackstone - Byron Wien
   Byron's Ten Surprises for 2018
9. Stratfor
   Annual Forcast- Top 2018 Risks
10. PWC CEO Survey
    CEO Survey 2017- Top Risks 2018
11. PWC
    Top Policy Trends of 2018
12. PWC
    Top 10 AI tech trends for 2018
13. Willis Towers Watson
    2018 Emerging Risks
14. Reuters
    Breakingviews/Reuters Predictions 2018
15. IHS Markit
    2018 Predictions
16. CFR
    Preventive Priorities Survey 2018
17. Economist Intelligence Unit
    Top Global Risks June 2018
18. Top Teny
    Top 10 Risks the World Faces in 2018
19. Deloitte
    The Future of Risk: 10 Trends that will Affect the Future
20. BLG
    TOP LEGAL RISKS FOR BUSINESS IN 2018
21. DTCC
    DTCC SYSTEMIC RISK BAROMETER 2018 Risk Forecast
22. Risk.Net
    Top Operational risks for 2018
23. Threat Metrix
    Beyond Digital Identity: 2018 Predictions
24. Stroz Friedberg , Aon Company
    2018 Cybersecurity Predictions A Shift to Managing Cyber as an Enterprise Risk
25. Aon Risk Solutions
    Global Risk Management Survey 2017/18
26. Aon Risk Map
    Political Map
    2018 Political, Risk, Terrorism, and Political Violence Map
    Aon Terrorism & Political Violence Themes 2018
27. Communications Today
    Global Risk Management Survey 2018, Aon Risk Solutions
28. The Grey Rhino
    Top Global Gray Rhinos of 2018