

Cybersecurity 101: "An Ounce of Prevention is Worth a Pound of Cure"

by Rois Ni Thuama

A Doctor of Law and subject matter expert in cyber governance and risk mitigation, Rois is Head of Cyber Security governance for Red Sift one of Europe's fastest-growing cybersecurity companies. Working with key clients across a wide market spectrum including legal, finance, banking, and oil & gas Rois writes and presents on significant cyber threats, trends, addressing and managing risks.

High profile data breaches have brought Facebook, British Airways and Equifax into the media spotlight, resulting in both media and consumer backlash and a good deal of negative shareholder attention.

It is unsurprising then that the reputational damage and business disruption that followed these incidents has created a sense of urgency for board members to review their cybersecurity policies, products and spending.


Not only will directors want to ensure that they are protecting their firms' digital assets, commercially sensitive information & personally identifiable information (PII) amongst other things, but they will undoubtedly want to protect themselves against shareholder reaction and litigation.

The operational impact, media coverage and consumer backlash, together with record fines as a result of breaches of the General Data Protection Regulation (GDPR), have doubtless contributed to the

increased spend. The fact that directors have a legal obligation to their company to exercise reasonable care, skill and diligence clearly informs their view and their appetite for sensible security measures. What is meant by 'sensible security measures' can be summed up with the old adage, an ounce of prevention is worth a pound of cure. So, it is entirely foreseeable that firms would rank protective cybersecurity products & services more highly than those services that offer remediation.

ACCOUNTANCY | PLANNING | ADVICE

ifac



Grow your career with us

If you have the drive and motivation to succeed, then all you need is the opportunity to grow. At *ifac* we have openings for a range of roles at all career stages - from graduates to experienced professionals.

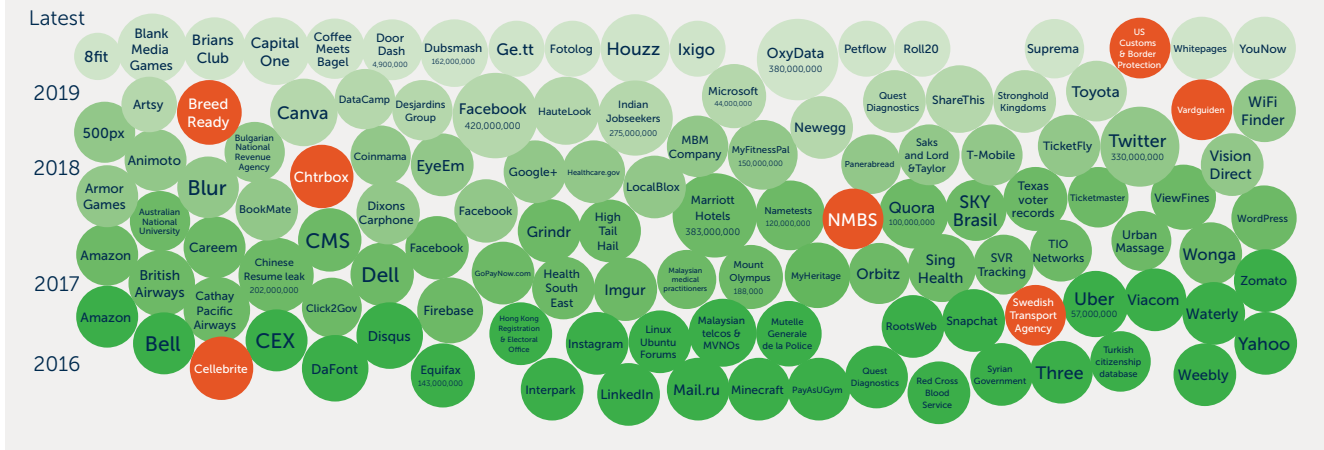
Grow your career as part of a dynamic top ten firm. We are currently recruiting for:

- Tax Senior, Dublin
- Senior Accountant, Enniscorthy
- Senior Accountant (Partner Fast-Track), Trim

For more information and to see how you can become part of our team, visit www.ifac.ie/about/careers

World's Biggest Data Breaches & Hacks Jan 2020

Source: informationisbeautiful.com



The expectation within the cybersecurity industry is that the current trend for spending on cybersecurity products and services will continue to increase and is expected to exceed \$1 trillion cumulatively over the five-year period from 2017 to 2021. To put that into context, the aggregate spend globally for cyber security in 2004 was \$3.5 billion.

In 2018, JP Morgan CEO Jamie Dimon wrote in the 2018 Annual Report that the firm spends nearly US\$600 million a year to protect their business. That's a single business with a cyber security budget that 14 years previously would have represented a 1/7th of the total global spend. If you're not wide-eyed reading that, go back and read it again.

But there's more, take a look at an excerpt from the annual report.

The threat of cyber security may very well be the biggest threat to the U.S. financial system.

I have written in previous letters about the enormous effort and resources we dedicate to protect ourselves and our clients - we spend nearly \$600 million a year on these efforts and have more than 3,000 employees deployed to this mission in some way.

This short paragraph reveals two things:

1. A willingness to spend significant sums to protect assets and client's privacy.
2. An error. The headline in bold refers to the 'threat of cyber security' which is obviously not right. The author(s) must have intended to refer to cyber threats. In all likelihood it should have read 'Cyber threats may very well be the biggest threat to the U.S. financial system'.

There are a number of reasons why all of this information should matter to accountants.

1. Increased oversight -

As cybersecurity budgets balloon, this will be required. Some cybersecurity products are so expensive that a compelling business case will need to be made at board level and will merit a discussion. Accountants familiar with good governance principles specifically the 'four-eyes' principle will desire a robust business justification for a material spend. No one in a business should have carte blanche to sign off huge sums. To that end, it is imperative that accountants, auditors, CFO's, etc. are able to participate in the conversation by:

- a. understanding the business case,
- b. being able to sensibly interrogate that business case,

c. learning to rely on their internal cyber and information security experts.

It is worth pointing out that reasonably priced cybersecurity products which address significant cyber threats would not merit such attention from the board. These 'no-brainer' solutions should be signed off without conversation on the advice of the firm's cyber and information security experts. Not every cyber matter merits a lengthy inquiry and trusting your experts saves your firm money and time.

2. Errors -

Often, these appear in cybersecurity literature. JP Morgan is a sophisticated, innovative firm. They are undoubtedly a global leader in terms of their cybersecurity posture. However, despite this level of sophistication, this report to their shareholders contains a glaring error, as discussed above. Cybersecurity isn't the threat, it's the solution. Just keep this in mind, if something doesn't make sense to you, it might not be you.

3. Career advancement -

By 2022 the EU will not be able to fill 355,000 jobs in the cyber security sector. For anyone wanting a career change or accelerated career advancement, they should consider some additional cybersecurity training to gain a better understanding of essential products and policies.

Understanding the business case

It's frequently said in cyber that the offence informs the defence. Indeed, it's a sensible rule to live by. But to deploy it, you must first understand what the offences are (i.e. threats), and then determine which offences/threats are the most significant. In order to do that, you will need to have at least a passing familiarity with the cyber threat landscape which organises the offences in a clear way.

For this, an excellent starting point was provided by Prof. Wall, Head of Law School at Leeds University, a leading cybersecurity academic. His matrix distils cybercrimes into their component parts so that every cybercrime fits into a set description. By knowing where the threat sits, you are more easily able to determine the solution.

Cyber threat landscape

For example, certain cybercrimes do not need a technical or expensive solution. Firms can protect their reputation from damaging social media comments (i.e. hate speech or defamatory remarks) by ensuring that employment contracts have carefully crafted provisions that encourage compliance to a well-formed cyber governance policy. The key is not to deploy expensive technical solutions simply because the crime occurs on a computer. The answer might be a written process, policy or carefully crafted provision in a contract.

Conversely, don't rely on policies when the problem is 'in the machine'. It is vital not to turn staff into filters and firewalls. No amount of training will assist staff in crunching through metadata, that is computational work and should be done by, you guessed it, computers. There are a number of downsides to expecting human resources to do computational work, including:

- i. burnout
- ii. decreased productivity
- iii. increased stress levels
- iv. failure
- v. employment tribunals

Crime Types →	Crime against machines/ integrity-related	Crime using machines/ Computer related	Crimes in the machine/ Content related
Opportunities ↓	Harmful/Trespass	Acquisition/(Theft/ Deception)	Onscenty/Violence
Cyber-Assisted Crimes Traditional crime using computers. More opportunities for traditional crime	<ul style="list-style-type: none"> Phreaking Chipping 	<ul style="list-style-type: none"> Frauds Pyramid Schemes 	<ul style="list-style-type: none"> Trading sexual materials Stalking Harassment (personal)
Cyber Enabled Crimes Hybrid cybercrime New opportunities for traditional crime (e.g. organisation across boundaries)	<ul style="list-style-type: none"> Cracking/Hacking Viruses Hactivism 	<ul style="list-style-type: none"> Multiple large-scale frauds 419 type fraud Trade secret theft ID Theft 	<ul style="list-style-type: none"> Online sex trade Camgirl sites General Hate speech Organised paedophile rings (child abuse)
Cyber-Dependent crimes True Cybercrime New opportunities for new types of crime (Sui Generis)	<ul style="list-style-type: none"> Spams (list construction and content) Denial of service Information Warfare Parasitic Computing 	<ul style="list-style-type: none"> Intellectual Property Piracy distribution Online Gambling E-auction scams Phishing, smishing, vishing 	<ul style="list-style-type: none"> Cyber sex Cyber-pimping Online grooming Organised Bomb talk / Drug talk / Targeted hate speech Social network media crimes

We're already seeing legal cases where human resources have been put under exceptional strain, leading to suffering with post-traumatic stress disorder (PTSD) because they have been expected to do the work of AI.

When we assess the entire picture, the first question to ask is: which of these *represents a significant cyber threat?*

This is typically where vendors will explain that their solution solves *the most significant* cyber threat. Now although that may be true, more often than not it's mere puff. This leads to the second question, that must be asked: *who is your source for that claim?*

If independent, trusted experts within the Intelligence Communities (IC) have warned from both perspectives that something is a significant cyber threat, that should be enough guidance for reasonable directors to move to the third question. Sensible, independent sources for cyber threat assessments include National Cyber Security Centre (NCSC), Federal Bureau of Investigations (FBI), Internet Crime Complaint Centre (IC3) and the Department of Homeland Security. There are other bodies, but this is a good starting point.

Let's take phishing/business email compromise (BEC) as an example. The IC on both sides have warned businesses that phishing emails/BEC are a significant cyber threat. The FBI refers to it as the US\$26 billion scam. The NCSC have warned about phishing and even put the legal sector in the UK on express notice that this is the most significant cyber threat facing law firms. Bad actors use phishing emails as their starting point for 70% of data breaches and 90% of targeted cyberattacks. It follows that if you fix phishing, you can remove the starting point for 70% of data breaches and 90% of targeted cyberattacks, therefore reducing the overall chances of these events happening.

This leads neatly to the third question: *is there an industry standard fix?*

For BEC/phishing attacks, there is. The solution to BEC is DMARC. DMARC is the global industry standard protocol recommended by Email Service Providers (ESPs) and government agencies. The protocol helps your computer to verify that the email you send from your business email address is authentic, protecting both your brand and your clients. This is why the IC in the US and Britain have repeatedly emphasized

the importance of deploying the DMARC protocol. For people new to cybersecurity, here's a neat hack: if you ever see something done at protocol level, its importance cannot be overstated. Protocols are the fundamental building blocks of the internet, it's the digital equivalent of underpinning a house. Failing to fix at protocol level means you are on shaky foundations.

To recap:

1. What's the problem?
2. Will trusted independent sources support the claim that it is a problem?
3. Is there an industry standard fix that is well known and understood?

After answering yes to those three questions, the final question to ask is whether it is reasonable and proportionate to deploy a fix it? For example, if the fix costs X times the total value of the firm, the answer will, of course, be no. If it's less than the cost of the Christmas party or what the office spends on non-essentials like plants or days away, the answer will undoubtedly be yes.

Now that we have a passing understanding of the cyber threat landscape and the questions a reasonable director would ask; it remains to review the risks.

Cyber risks

The major risks associated with cybersecurity failures are:

1. Business operational - the scale of the operational damage depends on the threat and what steps your information security team have taken to protect against it. It might result in a total cessation of business capabilities for minutes, hours, days or weeks.

2. Litigation - includes fines, legal costs and damages. By now everyone is familiar with the fine: up to 4% of global annual turnover or €20 million, whichever is higher. Less well known perhaps is that GDPR contains a provision which will give rise to claims from data subjects affected by data breaches. Some law firms have positioned themselves to respond quickly to data breaches by optimising keywords to drive web traffic to their website.

In the event of a data breach, these law firms, already highly ranked, will be returned for users on the first page on a Google search which will facilitate class actions, at speed. This will undoubtedly contribute to business disruption as senior management turns their attention and man hours away from production to damage limitation.

3. Reputational damage - studies indicate that public companies suffer a loss of 7% off their share price on the initial news shock, further amplified by 15-20% on additional news flows. However, the reality can be far worse than researchers initially evidenced. For example, in 2016 a BEC attack saw a French firm lose 20% off its share price in a single day. It started the day at €35 billion and, despite the firm's rapid response to a 'fake news' article, had €7 billion wiped off its price. It is of course not possible to measure the impact to a privately held firm, but we do know that a combination of factors, including the loss of earnings because of business disruption, leads to a reported 60% of firms folding within 6 months of an attack.

Conclusion

The decision-making process can be somewhat nuanced but ultimately, the process is more science than art. Businesses need to learn quickly that dealing with known cyber threats, which cybercriminals rely on, might not sound ground-breaking, but it is essential governance 101. If you're not fixing the known problems with well-known solutions, your firm's cyber security and risk posture is immature, indefensible and imperils the business and its staff.



Rois Ni Thuama

Doctor of Law and subject matter expert in cyber governance and risk mitigation. Head of Cyber Security governance for Red Sift.