Using cyber insurance to run virtuous circles around cyber risk

Dr Mike Lloyd

Dr Mike Lloyd, RedSeal

In 1789, Benjamin Franklin wrote to his friend, the French physicist and Encylopédiste Jean-Baptiste Le Roy: "Our new Constitution is now established, and has an appearance that promises permanency".[1] Then he added: "But in this world nothing can be said to be certain except death and taxes."

Now we know better, of course. The digital transformation attaches one more item to Franklin's list of certainties: digital data breach. In 2016, the Ponemon Institute, which conducts independent research on privacy, data protection and information security policy, concluded that each of the 383 companies it surveyed had a "26% probability of a material data breach involving 10,000 lost or stolen records" within the "next 24 months".[2] Work this out over the long term, not for two years but for the projected life of your business and you must accept the certainty of data breach just as you accept the certainty of death and taxes. Breaches will happen. They will happen to you.

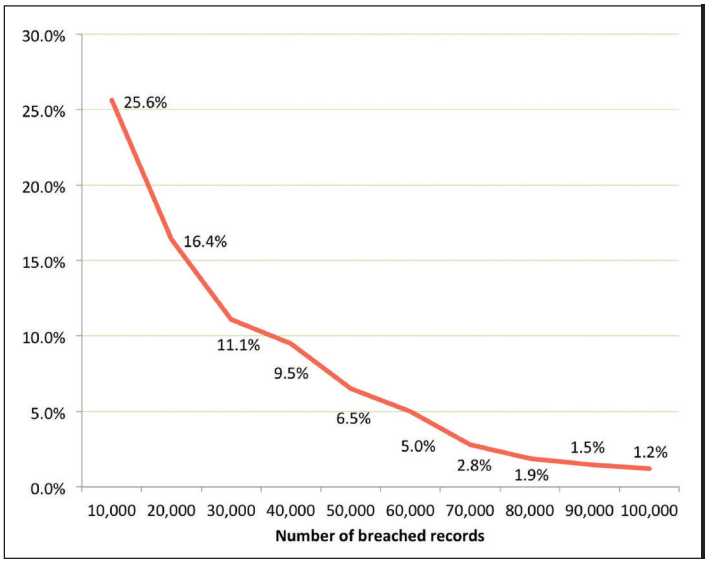
Acceptance not surrender

Acceptance of a certainty does not mean surrender to that certainty. Accepting the certainty of death, for instance, Benjamin Franklin sought nevertheless to manage even this 100% risk by supporting the 1759 launch of the first life insurance company in America, which bore the formidable moniker, 'Corporation for Relief of Poor and Distressed Presbyterian Ministers, and of the Poor and Distressed Widows and Children of Presbyterian Ministers'.[3,4] If you could not evade the certainty of death, at least you could insure against its financial consequences.

Eight years earlier, Franklin, who had founded the Union Fire Company to help fight fires in his hometown of Philadelphia, met with other such companies in the city to create the first mutual fire insurance company in America – another mouthful, "The Philadelphia Contributorship for the Insurance of Houses from Loss by Fire."[5-7]

As a charter member of his own Union Fire Company (founded in 1736), Franklin knew that the risk of conflagration in the mostly wood-built city of Philadelphia was, though not a certainty for each and every house, great. The genius of his company's business model was that Franklin and his partners did not just gamble that the buildings they insured would never burn down. Instead, they made the issuance of each policy contingent on their inspector's evaluation of your property. The inspector assessed aspects of construction and other elements in determining whether the house was a good risk for insurance. These factors came to constitute a *de facto* set of standards for building more fire-resistant structures.

The standards did not prevent all fires, of course, but they reduced the likelihood of fire and, even more important, improved the resilience of the insured houses. In the event of a fire, the houses that met the insurance company's standards were less likely to suffer catastrophic damage than those houses that did not make the cut. Thus, insuring the risk of fire reduced the risk of financial loss to the homeowner even as it reduced the risk of catastrophic fire itself – thus hedging the risk of financial loss to the insurance company. In this way, Franklin's company drew a virtu-



Probability of a data breach involving a minimum of 10,000 to 100,000 records. Source: IBM/Ponemon Institute.

ous circle. It provided insurance against fire loss, but only on condition that the insured house was built to make it less likely to burn and, if it did burn, less likely to burn to the point of total loss.

Franklin's business model also introduced another element into the insurance business. It assessed risk by means of an objective monetised metric. In effect, the Franklin model laid the foundation of actuarial science, which transformed risk from a crapshoot to a rational business decision.

Fully covered

"I think the cyber insurance industry has enormous potential to positively shape the cyber-security ecosystem in this country, as it has so many other things in this country – as it has with fire prevention, as it has with automobile safety," Richard Clarke, formerly US National Co-ordinator for Security, Infrastructure Protection and Counter-Terrorism, told attendees at 'Cyber Insurance and Its Evolving Role in Helping to Mitigate Cyber Risks', a 2017 forum cosponsored by the National Association of Insurance Commissioners (NAIC) and the Stanford Cyber Initiative.[8,9]

In the fullness of time, digital breaches are as certain today as death and taxes. Likewise, for any twenty-first-century business at any moment in time, a breach is at least as great a risk as fire was in Franklin's Philly. For all these hazards, analogue and digital, insurance seems the logical tool for managing risk.

But there are problems. To begin with, currently available cyber insurance barely begins to cover all costs associated with a breach. How could it? Insurers have yet to deploy technology and methodology to properly measure the risk they are being asked to cover. They focus on the external threat environment and not on the organisation's internal resilience, its ability to defend itself. They assess the external threats to the network, but not the network itself. It is as if Ben Franklin's insurance inspector made his coverage decisions on the basis of a look at the neighbourhood while ignoring the structure of the house that was up for a policy.

To make adequate cyber insurance cost-effective for the consumer and profitable for the insurer, we need what Franklin – and every successful insurance provider since – has had: a monetised metric by which to assess risk. Without an assessment of the network to be insured, however, insurers suffer from a "dearth of data". As Deloitte's Sam Friedman and Adam Thomas explain in 'Demystifying cyber insurance coverage', this dearth is one of four obstacles that inhibit insurers from meeting the demand for cyber coverage.[10] The other three are the fact that cyber-attacks keep evolving, that each breach has the unpredictable potential for catastrophic accumulation of loss, and that there is "tunnel vision in the coverages offered". Current policies usually cover only out-of-pocket costs associated with notifications and other statutory reporting and compliance. Better for a business owner to lose her factory to fire than to suffer a big-time breach. At least when a factory burns down, insurance will rebuild it, pay the lost wages of workers, cover inventory and may even cover lost revenues.

Identifying obstacles

Friedman and Thomas also identify obstacles from the perspective of the insured. Buyers understand neither their cyber risks nor their insurance options. Cyber risk is spread over a wide range of coverages and the available policies lack standardisation. Finally, the legal context defining cyber liability is unsettled and fluid. Taken together, these producer and consumer obstacles seem daunting indeed. But so was the prospect of a Philadelphia in flames. Like Ben Franklin, digitally intensive enterprises, the insurance industry and cyber-security providers need to resist panic, face the problem and work the problem.

First, before insurance consumers can make intelligent, cost-effective choices, they must have clarity from insurers. Clarity begins by replacing dearth with data, and that means evaluating both internal and external threats. These must be measured as objectively as possible using reliable, tested scoring methods. Once insight is gained into these risks, insurers and consumers must collaborate with IT and cyber-security professionals to rationally monetise the measured risks.

Now, here is where the lessons of Ben Franklin and 259 years of insurance industry experience come into play. Passive evaluation, measurement and monetisation are necessary but not sufficient. Armed with data, the insurance industry will be in a position to create the digital equivalent of Franklin's qualifying requirements for coverage-worthy home construction. To the extent that the availability of a cost-effective policy (or any policy at all) is made contingent upon evaluation of the digital resilience of an applicant's network, businesses will be incentivised to become more digitally resilient. The more resilient they are, the better the risk for insurers, who will be better enabled and motivated to provide fuller and more cost-effective coverage.

With coverage qualification and cost pegged to a measurement of resilience – the capacity of a network to resist, survive, and recover from attacks and breaches – those who insure the digital world will do what insurers of the physical world have long been doing. They will create a virtuous circle by which their products will de-risk financial loss even as they de-risk the potential sources of that loss by incentivising the creation of more resilient networks.

Over time, the circle will grow evermore virtuous. By working together, insurers, businesses, and cyber-security providers will create the conditions in which the adoption of cyber insurance becomes increasingly widespread, thereby permanently transforming our digital environment into a safer, less costly and more cost-effective space in which to live and do business.

About the author

Dr Mike Lloyd is the chief technology officer at RedSeal. He has more than 25 years experience in the modelling and control of fast-moving, complex systems. He has been granted 21 patents on security, network assessment and dynamic network control. Before joining RedSeal, Lloyd was CTO at RouteScience Technologies (acquired by Avaya), where he pioneered self-optimising networks. He served as principal architect at Cisco on the technology used to overlay MPLS VPN services across service provider backbones. He joined Cisco through the acquisition of Netsys Technologies, where he was the senior network modelling engineer. Lloyd holds a degree in mathematics from Trinity College, Dublin and a PhD in stochastic epidemic modelling from Heriot-Watt University, Edinburgh.

References

1. 'Death and taxes (idiom)'. Wikipedia. Accessed Aug 2018. https://en.wikipedia.org/wiki/Death_and_taxes_(idiom).
2. '2016 Ponemon Cost of Data Breach Study'. IBM/Ponemon Institute, 2016. Accessed Aug 2018. https://www-03.ibm.com/security/ca-en/data-breach/.
3. 'Presbyterian Minister's Fund Records'. The Historical Society of Pennsylvania, 2008. Accessed Aug 2018. http://hsp.org/sites/default/files/legacy_files/migrated/findingaid-3101presbyministers.pdf.
4. Newman, Frank. 'The acquisition of a life insurance company'. The Business Lawyer, vol.20, no.2, Jan 1965, pp.411-416. Accessed Aug 2018. www.jstor.org/stable/40683978?seq=1#page_scan_tab_contents.
5. 'In case of fire'. US History. Accessed Aug 2018. www.ushistory.org/franklin/philadelphia/fire.htm.
6. 'Insurance Ben-efactor'. PBS. Accessed Aug 2018. www.pbs.org/benfranklin/l3_citizen_insurance.html.
7. Beattie, Andrew. 'The History of Insurance in America'. Investopedia, 8 Jun 2018. Accessed Aug 2018. www.investopedia.com/articles/financial-theory/08/american-insurance.asp.
8. O'Connor, Amy. 'Former U.S. Security Expert: 5 Ways the Insurance Industry Can Improve Cybersecurity'. Insurance Journal, 6 Nov 2017. Accessed Aug 2018. www.insurancejournal.com/magazines/features/2017/11/06/469993.htm.
9. 'Cyber Insurance and Its Evolving Role in Helping to Mitigate Cyber Risks'. National Association of Insurance Commissioners, 11 Oct 2017. Accessed Aug 2018. www.naic.org/documents/cipr_events_stanford_cyber_agenda.pdf.
10. Friedman, Sam; Thomas, Adam. 'Demystifying cyber insurance coverage'. Deloitte, 23 Feb 2017. Accessed Aug 2018. https://dupress.deloitte.com/dup-us-en/industry/financial-services/demystifying-cybersecurity-insurance.html

The best form of defence – the benefits of red teaming

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, *Computer Fraud & Security*

One of the best ways to understand how well your defences would withstand a cyber-attack is, in fact, to come under attack. Nothing exposes your weaknesses better than having them revealed by skilled hackers. That's the idea behind penetration testing. However, if you have systems or information assets you know are especially valuable, you might want to consider ramping things up a notch and engage in red teaming exercises, as Gemma Moore, a director at Cyberis, explains in this interview.

The key difference between penetration testing and red teaming is one of focus, says Moore. "When you're doing a penetration test of a system, you're looking at trying to get full coverage of the technical vulnerabilities within the defined scope of work," she says. "So if you're looking at an application, you're looking to find all the vulnerabilities of whatever type that are present within that application. If you're looking at the network, you're looking at finding all the vulnerabilities that you can exploit."

A red team exercise, on the other hand, is objective-led – and Moore thinks 'simulated attack' is a term that more accurately reflects this, although 'red-teaming' is more widely adopted in the industry. "Instead of saying, what are all the technical vulnerabilities in this application, you're answering questions such as, how could I use this application to get hold of a piece of valuable data – a critical customer database, perhaps. So the questions you're asking are very different."