Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

06: Case Studies and Research

Date

UWE Bristol | University of the West of England

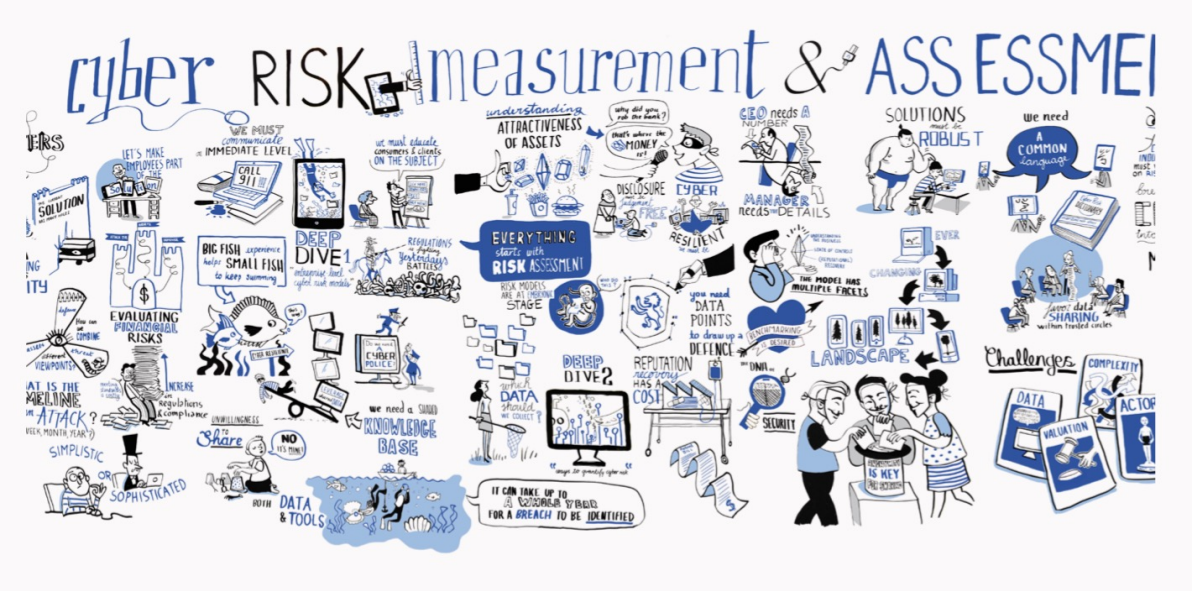
Today

- Let's look at some recent white papers and research on Cyber Risk
  - Cyber Value-at-Risk (FAIR is one model for performing CyberVaR)
  - Challenges in Quantifying Impact – Deloitte
  - Evaluating Residual Risks – Oxford

Quantifying Risk

- World Economic Forum
- Partnering for Cyber Resilience, Towards the Quantification of Cyber Threats Report

- Original report that proposed the need for Cyber Value-at-Risk models



UWE Bristol University of the West of England

Cyber VaR

The cyber value-at-risk model helps answer the following cyberattack questions for stakeholders:

- **Who and why?** Addresses threat types executing
  the attack scenario in terms of target attractiveness (encompassing threat motivations and exposed target characteristics)
- **What and how?** Addresses the type of attacks applied (in terms of technical means and level of sophistication)
- **Where and when?** Addresses vulnerability as per a standard cyber resilience maturity level measure

Cyber VaR

Feedback was gathered concerning key desirable attributes for a shared model. The attributes include:

Applicability

Ability to apply the model across different industries, organizations and adjust it depending on the needs of the company

- Generic applicability across industries
- Scalable to address differing level of maturity
- Suitable for customization
- Ease of interpretation
- Traceable and transparent

Precision

Comprehensiveness and measurement accuracy of the model

- Balances generalizability, accuracy and precision
- Practical concerning data availability

Timeliness

Ability to timely reflect the environment around incidents

- Ability to track previous incidents/cyber events
- Timely in tracking present and emerging risks

Scope

Ability to cover a wide range of factors and risks

- Provides for a market valuation of risk
- Complete in addressing internal and external risks
- Addresses both tangible and intangible risks

Decision-making process

Potential to serve as an effective risk measurement tool for executives and decision-makers

- Assists in supporting investment decisions
- Focuses on preserving value in the face of pervasive threats
- Compatible with existing enterprise risk management frameworks
- Establishes a foundation for cyber risk transfer markets and instruments

Cyber VaR

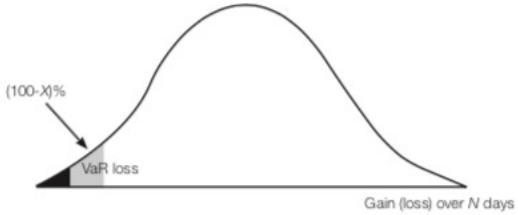
While the Initiative identified more similarities than differences among cyber risk models, a number of challenges were also identified. They include:

- Data availability and standardization, specifically concerning historical data on threats and breaches (in most industries there is no common information sharing standards or platforms, outside of financial services industry)
- Damage valuation standardization, including tangible and intangible assets, i.e. reputation and brand (measuring of the effects of cyber incidents against those assets is not standardized)
- Willingness to share information across companies (companies are unwilling to share information due to reputational and regulatory risks and due to the risks of misuse of information)
- Information asymmetry due to limited visibility into a company's cyber resilience (various executive functions within an organization have a different outlook on the maturity of their company in terms of security posture
- Matching between actual risks versus measured risks (the need for less error-prone models for assessing security posture)
- "Chicken and egg" challenge of risk transfer markets both requiring and justifying quantification efforts (insurance companies would like to offer competitive market solutions to offset cyber risks, but they do not have the necessary data to build these solutions; they do not have the data because they do not have ways of collecting it, e.g. by offering products in exchange for data).

UWE Bristol | University of the West of England

What is Cyber VaR?

- The concept of cyber value-at-risk is based on the notion of value at risk, widely used in the financial services industry. In finance, VaR is a risk measure for a given portfolio and time horizon defined as a threshold loss value. Specifically given a probability X, VaR expresses the threshold value such that the probability of the loss exceeding the VaR value is X. In figure 2, the curve is the normal distribution of the risk, N days is the time horizon, the X axis is the performance of the portfolio and X represents the VaR threshold. (100 – X)% is the probability of not exceeding the VaR value



It is important to note that in this report we specify properties that VaR should have, but not specifically how to compute it. Cyber value-at-risk could be successfully applied to cyber risks as a proxy concept for risk exposure and could appeal to a wide range of industries and enterprises. This cyber risk model uses the probabilistic approach to estimate the likely loss from cyberattacks over a given period.

Cyber value-at-risk requires organizations to understand the key cyber risk drivers (or components) required for modelling cyber risks, and the dependencies between these components which can be embedded in a quantification model. As an outcome, a complete and complex cyber value-at-risk model will help organizations answer address the following:

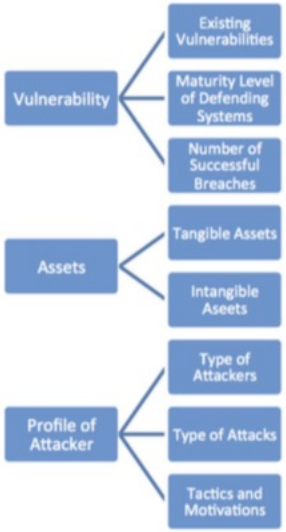
Given a successful cyberattack, a company will lose not more than X amount of money over period of time with 95% accuracy.

UWE Bristol | University of the West of England

What is Cyber VaR?

The goal of cyber value-at-risk is to standardize and unify different factors into a single normal distribution that can quantify the value at risk in case of a cyberattack. The effort should both be specific to the organization and reflect industry-wide trends. Once there is a statistical model to measure cyber risks, it can be incorporated into a broader risk strategy of a company.

Figure 3. Cyber value-at-risk components



Component 1: Vulnerability
There are the potentially less protected assets and systems that can become target of the attacks
- *Existing vulnerability:* Number of unpatched vulnerabilities, ratio of newly discovered vulnerabilities per each product used in the network, success rate of compromises per each machine during internal and external assessments
- *Maturity level of defending systems:* Number of security updates, number of defensive software components installed in the network, number of previous compromises, network typology and infrastructure

Component 2: Assets
At the core of cyber value-at-risk is high-level identification of assets under threat. This varies by organization, but typically includes tangible assets (e.g. funds and financial instruments, infrastructure, and production capabilities) as well as intangible assets (e.g. knowledge, privacy data, reputation, trust, brand, etc.) and structure assets (e.g. processes or systems that could get disrupted)
- *Tangible:* Costs of temporary of business interruption, complete business interruption, regulatory fees
- *Intangible assets:* Costs of temporary of business interruption, complete business interruption, lost IP, reputation loss

Component 3: Profile of attacker
The profile of adversaries targeting valuable assets
- *Type of attackers:* State-sponsored vs amateur, sophistication level of attackers (not so sophisticated, sophisticated, very sophisticated)
- *Tactics and motivation:* Number of novel attacks used, tends to be destructive (yes/no), tends to steal information (yes/no)

UWE Bristol | University of the West of England

See the WEF report for more detail

Quantifying Risk

- The benefits and limits of cyber value-at-risk
- Deloitte
- https://www2.deloitte.com/lu/en/pages/risk/articles/benefits-limits-cyber-value-at-risk.html

One of the biggest challenges associated with obtaining accurate results from cyber value-at-risk is the ability to estimate the probability of a successful attack

Beneath the Surface of a Cyberattack

A deeper look at business impacts

Deloitte

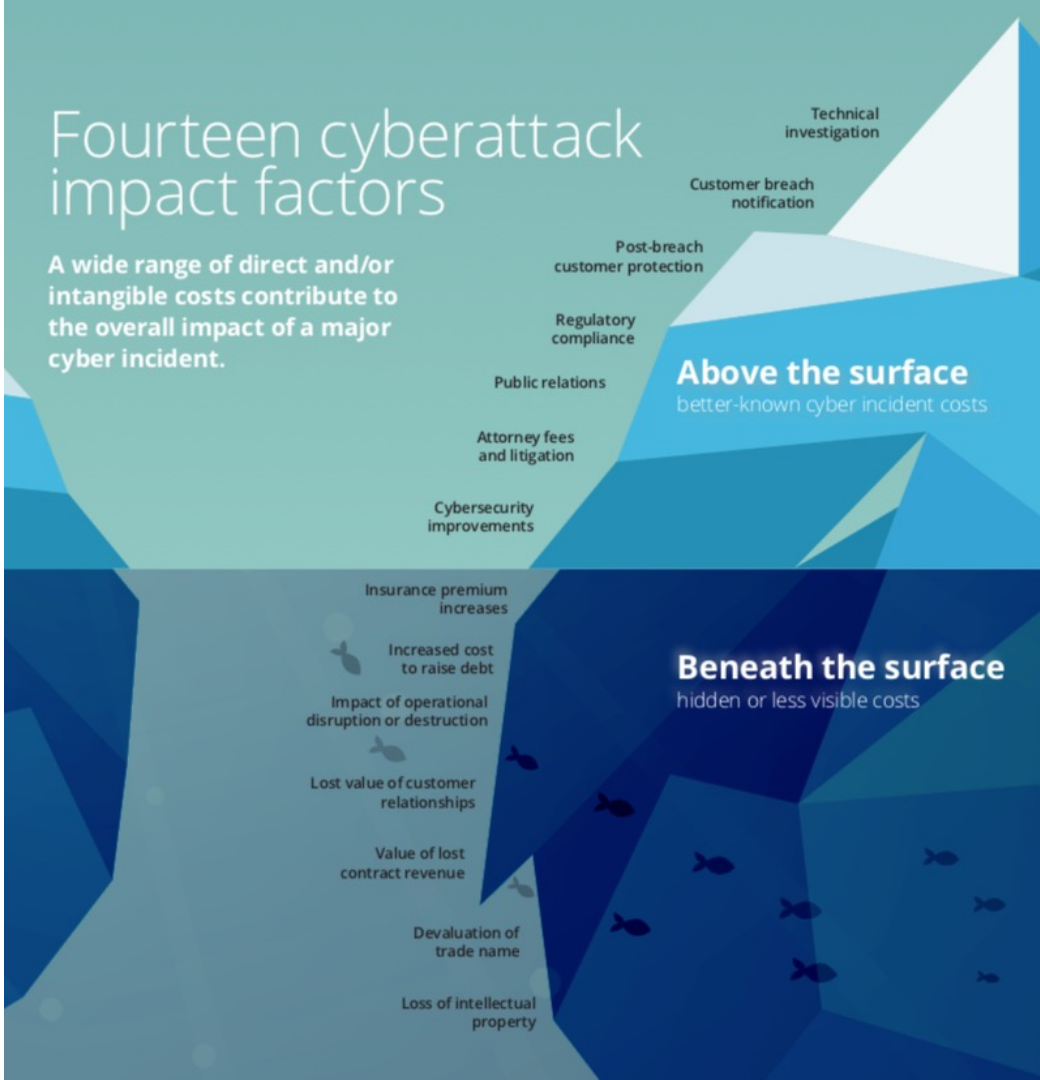
https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Above or Beneath the Surface

> What does a cyberattack really cost? Regulatory fines, public relations costs, breach notification and protection costs, and other consequences of large-scale data breaches are well-understood. But the effects of a cyberattack can ripple for years, resulting in a wide range of "hidden" costs—many of which are intangible impacts tied to reputation damage, operational disruption or loss of proprietary information or other strategic assets.

UWE Bristol | University of the West of England

Above or Beneath the Surface



UWE Bristol | University of the West of England

Scenario1: Health Insurer

About the company

- $60 billion annual revenue
- 50,000 employees
- 23.5 million members across the US (60 percent subscribed through employer contracts)
- Uses a patient care application, which provides medical alerts and allows health practitioners across its provider network to access patient records and insurance coverage information
- Holds open enrollment (the annual period when people can enroll in health insurance plans) November through January
- Regulated by both state and federal authorities
- Plans to raise $1 billion in debt capital to acquire a health system
- Pays $7 million annual premium for a $100 million cyber insurance policy

Scenario1: The Incident

- *In May, the company learned that a laptop containing 2.8 million of its personal health information (PHI) records had been stolen from the company's health care analytics software vendor. The compromise was revealed five days later when the company was notified by a corporate client that information associated with some of the client's employees had been listed for sale on cybercrime "dark web" sites. Concurrently, administrators of the patient care application began to notice a significant increase in the number of new user accounts created and in active use. They also detected that an additional one million patient records had been downloaded from the application database and were unable to confirm it was for authorized use. As a result, the company shut down physician access to the patient care application and activated its cyber incident response team. The application was kept offline for two weeks while the incident was investigated. During this time, coverage and claims validation between the company and its physicians and providers had to be done manually, requiring help from a professional services organization to provide "surge support" in the company's call center. Technical investigation revealed that cyberattackers had gained access to the patient care application using privileged credentials from the stolen laptop and had created a significant number of user IDs. Consequently, before service could be restored, new user accounts had to be issued for all application users, and new application and system controls were put in place.*

Scenario1: The Aftermath

- In the short term, core business functions were disrupted by the shutdown of physician access to the patient care application. While the application was unavailable, physicians and providers relied on less effective and efficient means of receiving medical alerts, increasing risk to patients. Without full access to health insurance coverage information, physicians and providers could not be certain of the financial implications—to both their institution and their patients—associated with the choice of care they provided.

- As the incident unfolded, impact to reputation and damage to trade name mounted. Lack of confidence in the company's data protection practices resulted in the loss of customers for approximately three years as some corporate clients and individual subscribers chose other health plan alternatives. Higher borrowing costs resulted in the delay of a strategic acquisition and, most impactful, the incident forced the company to mitigate reputation damage and member loss by reducing its annual premium increase over a five-year period. The company faced ongoing scrutiny for its handling of the incident; many months after the breach their cyber insurance premiums were raised and legal fees accumulated as the company faced identity theft lawsuits.

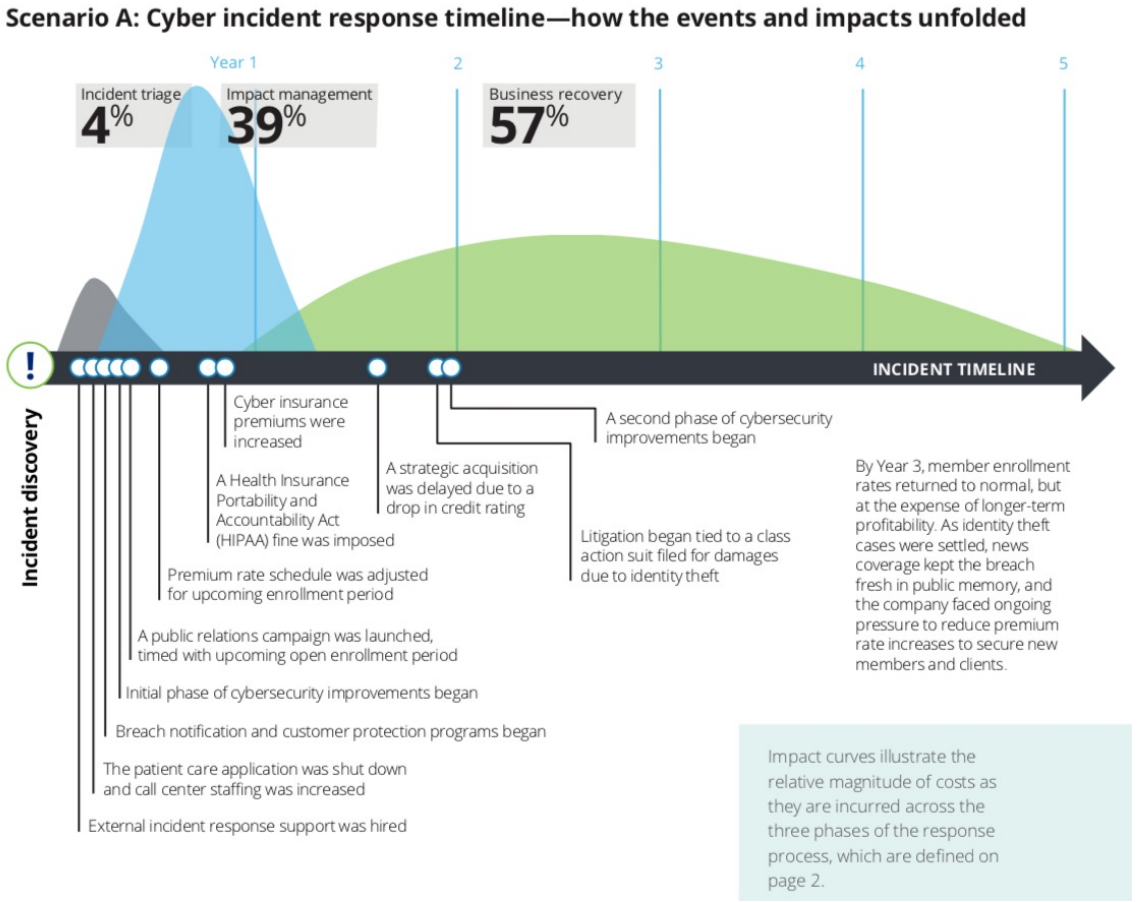
Scenario1: Cost of Impact

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

UWE Bristol | University of the West of England

Scenario1: Cyber Response Timeline



UWE Bristol | University of the West of England

Highlights of Business Impact

- The total cost of this cyberattack was greater than $1.6 billion over a five-year timeframe, and of significant interest, only 3.5 percent of the impact was accounted for "above the surface." To the casual observer, this incident was a classic example of PHI data theft, and while the company suffered common ramifications of a data breach, including customer notification, customer protection, and regulatory fines, there were much deeper implications. In reality, over 96 percent of the impact was "beneath the surface." What's more, almost 89 percent of the impact was associated with just three "beneath the surface" impact factors: value of lost contract revenue; devaluation of trade name; and lost value of customer relationships.

- Another interesting observation is how the impact played out over time. The immediate costs to "stop the bleeding" in the triage phase accounted for less than 4 percent of overall financial impact. Impact during the impact management phase jumped to nearly 40 percent. But that meant that approximately 57 percent of the impact played out in the years following the incident, challenging thinking that the year after an incident is the most impactful. In this scenario, the largest impacts were less obvious factors that played out over time.

Scenario2: Tech manufacturer

About the company

- $40 billion annual revenue
- 60,000 employees
- Growth strategy rests on innovation to support the management of Internet of Things (IoT) environments
- Holds hundreds of contracts with clients across multiple industries, including several very large federal government contracts
- Operating profit margin prior to the incident is 12.2 percent
- Pays $3.75 million annually for $150 million in cyber insurance

Scenario2: The Incident

- *After significant research, development, production, and marketing, the company was six months from a major release of a core product line that supports IoT environments. Earlier versions were deployed in the field for over 12 months across the government, transportation, utilities, smart home, and smart city sectors, and among service providers who support customers in those sectors. The company was informed by a federal agency that the company's infrastructure was breached by a foreign nation-state. An investigation revealed exfiltration of IP related to multiple product lines and confirmed that 15 of the company's 30 device product lines were impacted. Revenue associated with impacted product lines was projected to be 25 percent of total revenue over the following five years. Despite efforts to keep the incident confidential, 30 days after discovery a tech blog revealed that the foreign entity may be reverse-engineering the company's IoT products.*

Scenario2: The Aftermath

- The adversary's full intent was not known, but the company was concerned that counterfeit products could directly impact long-term sales and margins. It was equally concerned that attackers would exploit product vulnerabilities, or implant malicious code into their products. To be associated with future customer security incidents could be devastating to the company's reputation.
- While the company was largely able to recover within five years, the incident had a number of serious consequences. Sales and shipment of affected products were suspended for four months while security vulnerabilities were addressed. When word of the incident surfaced, a large government contract was terminated, causing an additional 5 percent drop in revenue. Significant unplanned costs were incurred, including costs to redesign security features and firmware for many product lines, and to redesign future products to embed advanced anti-counterfeiting software and hardware.
- The loss of IP related to multiple product lines was a significant blow to the organization and required unanticipated research and development (R&D) expenditures and product fixes. It was a full year before product sales returned to normal. Loss in market confidence lead to abnormally high sales force turnover. This type of business disruption across multiple functions caused a significant decline in operating efficiency. To help prevent future incidents, the company made security improvements to its corporate environment a top priority, including infrastructure upgrades and a data loss prevention program.

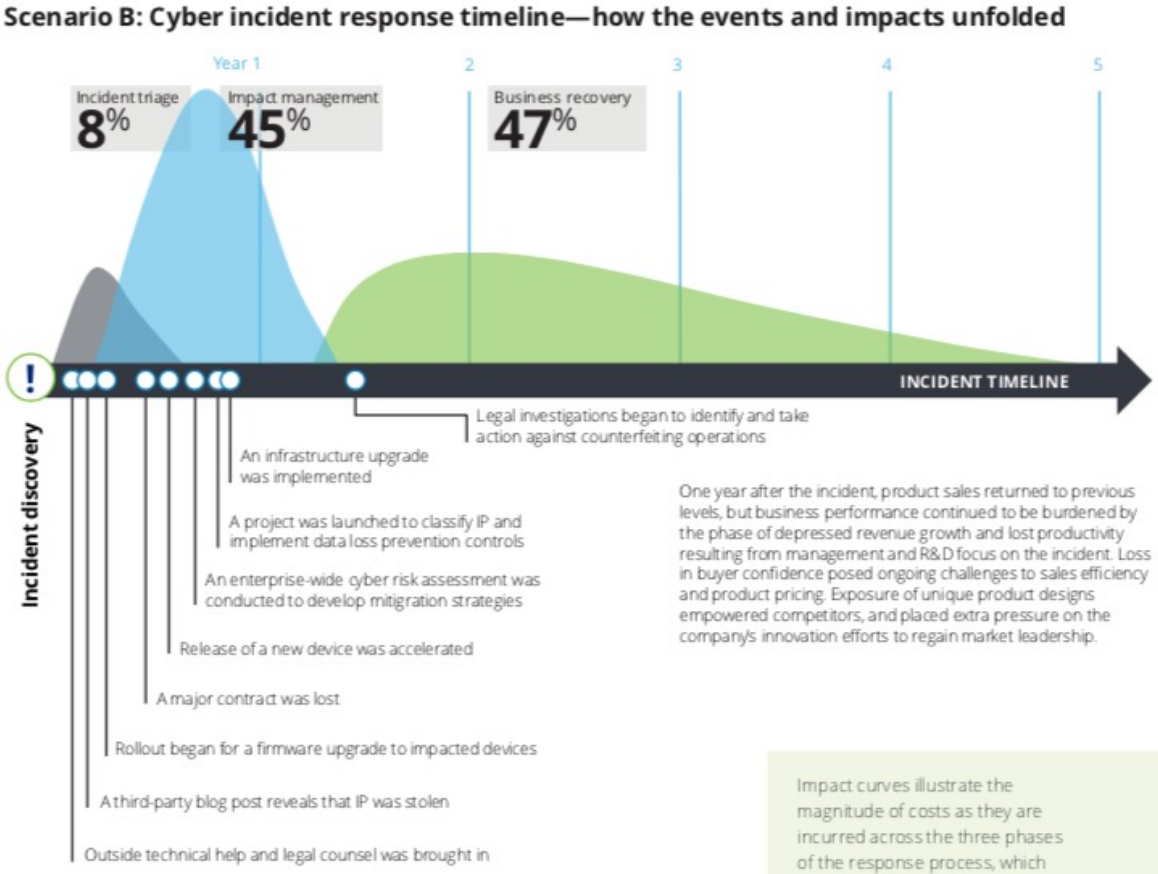
Scenario2: Cost of Impact

Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Cybersecurity improvements	1 year	13.00	0.40%
	Attorney fees and litigation	5 years	11.00	0.35%
	Public relations	1 year	1.00	0.03%
	Technical investigation	9 weeks	1.00	0.03%
	Customer breach notification	Not applicable	-	0.00%
	Post-breach customer protection	Not applicable	-	0.00%
	Regulatory compliance	Not applicable	-	0.00%
Beneath the surface	Value of lost contract revenue	5 years	1,600.00	49.11%
	Operational disruption	2 years	1,200.00	36.83%
	Devaluation of trade name	5 years	280.00	8.59%
	Loss of intellectual property	5 years	151.00	4.63%
	Insurance premium increases	1 year	1.00	0.03%
	Increased cost to raise debt	Not applicable	-	0.00%
	Lost value of customer relationships	Not applicable	-	0.00%
	Total		**$3,258.00**	**100.00%**

UWE Bristol | University of the West of England

Scenario2: Cyber Response Timeline



UWE Bristol | University of the West of England

Highlights of Business Impact

- In this incident, which could be categorized as a case of IP theft, the overall damage across all impact factors exceeded $3.2 billion over a five-year timeframe. Notably, the vast portion of the impacts were "beneath the surface;" those "above the surface" accounted for less than 1 percent of the total. In fact, 99 percent of the impact was focused in four areas: devaluation of trade name; value of lost contract revenue; operational disruption; and loss of IP.

- In terms of how the impacts played out over time, only 8 percent of the total impact fell within incident triage. Over 40 percent occurred during impact management, when operational disruption implications peaked, contract loss kicked in, and the company started to see the impact of lost IP. Interestingly, the largest impact was felt during business recovery, with half of the total impact having occurred more than two years following the incident.

Evaluating Residual Risks

- **"What do we do once we have deployed our best controls?"**

- *Watch CyberSA 2018 Keynote: https://www.youtube.com/watch?v=o1IgAgnwP2Y*
- *Slides: https://blackboard.uwe.ac.uk/bbcswebdav/pid-6741327-dt-content-rid-14637214_2/courses/UFCFWN-15-M_18jan_1/Keynote_Sadie_Creese_Cyberscience2018-3.pdf*

Combining Frameworks

- Chief Security Officer at Cimpress discusses the combination of NIST-CSF (Cyber Security Framework) with the FAIR analysis model: https://www.forbes.com/sites/forbestechcouncil/2019/01/02/two-frameworks-for-securing-a-decentralized-enterprise/#72940e0a5b52

- National Institute of Science and Technology – Cyber Security Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf