Lessons from Norsk Hydro on Loss Estimation and Cyber Insurance

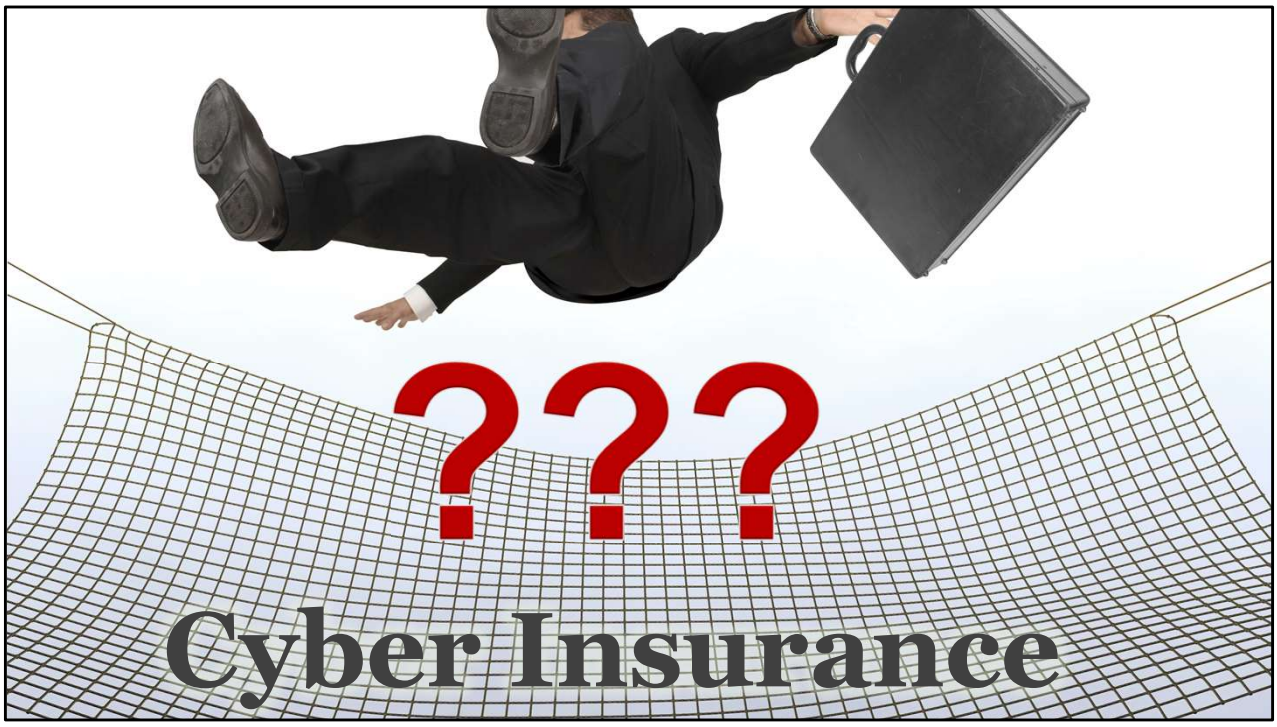
Russell Cameron Thomas
Principal Modeler for Cyber Risk
Risk Management Solutions, Inc. (RMS)

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved. January 21-23, 2020 1

Hello!

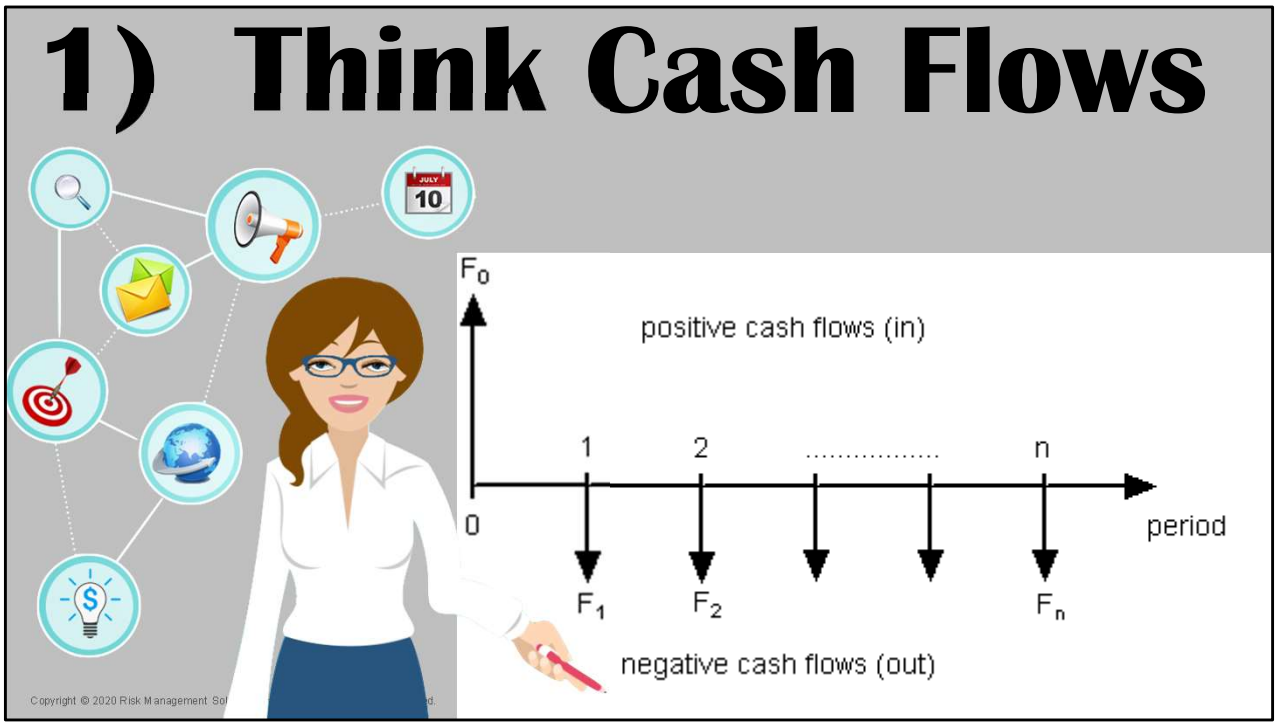
RMS is in the business of providing catastrophe risk models to the insurance industry – mostly Earthquakes, floods, hurricanes, fire, and similar. I work as a Principal Modeler on the Cyber Risk team, one of our newer products.

In the next 30 minutes we are going to use the Norsk Hydro ransomware breach as a case study to help you estimate breach impact



We will also look at cyber insurance to see how much of a financial safety net it provided.

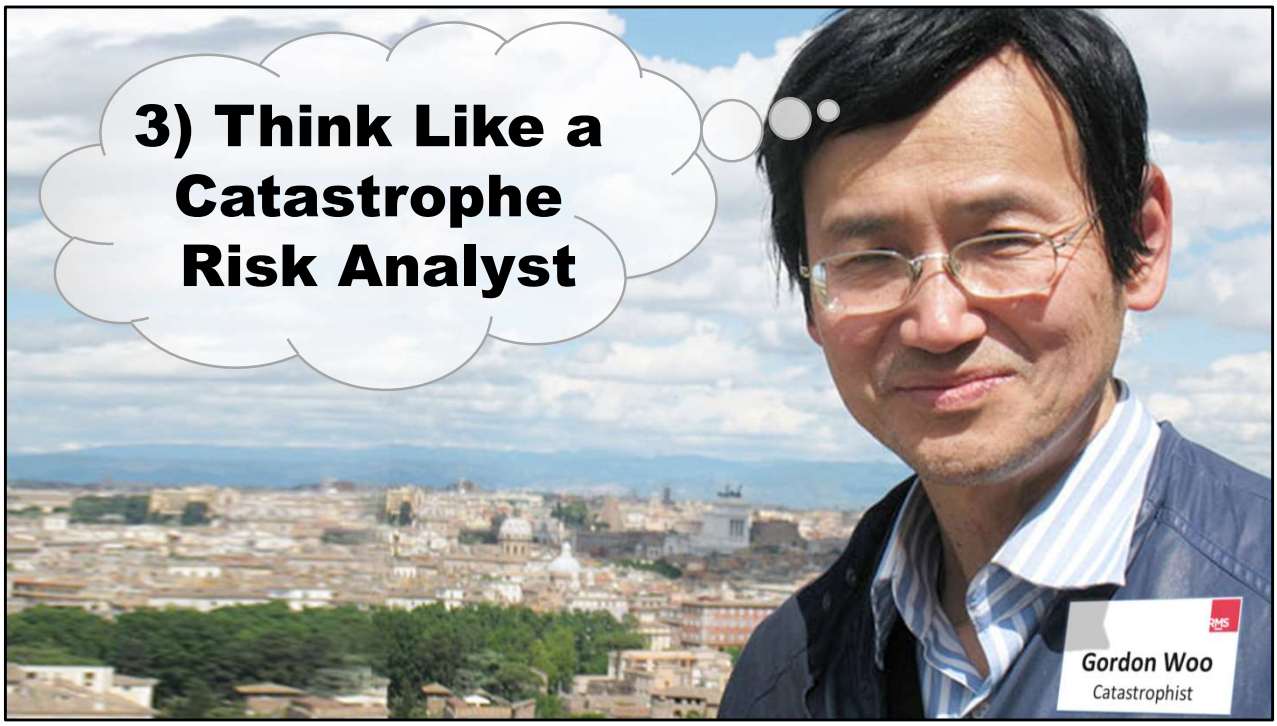
Here's a preview of the main messages



First – Think cash flows. Specifically – discounted cash flows

2) Think Bow Ties

Second – Think bow ties



Third – Think like a catastrophe risk analyst

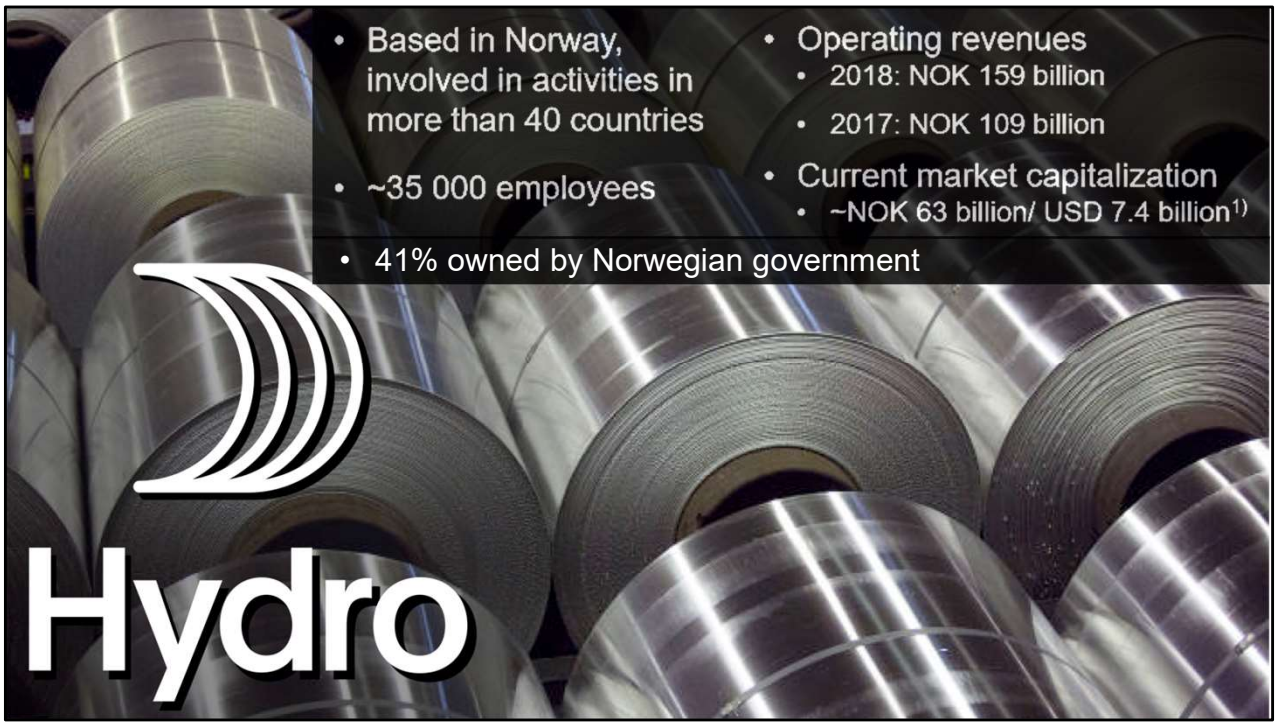
4) Fragility Matters

Fourth – Fragility matters

5) Cheese with holes can still be good

Copyright © 202

Finally – Cheese with holes can still be good cheese

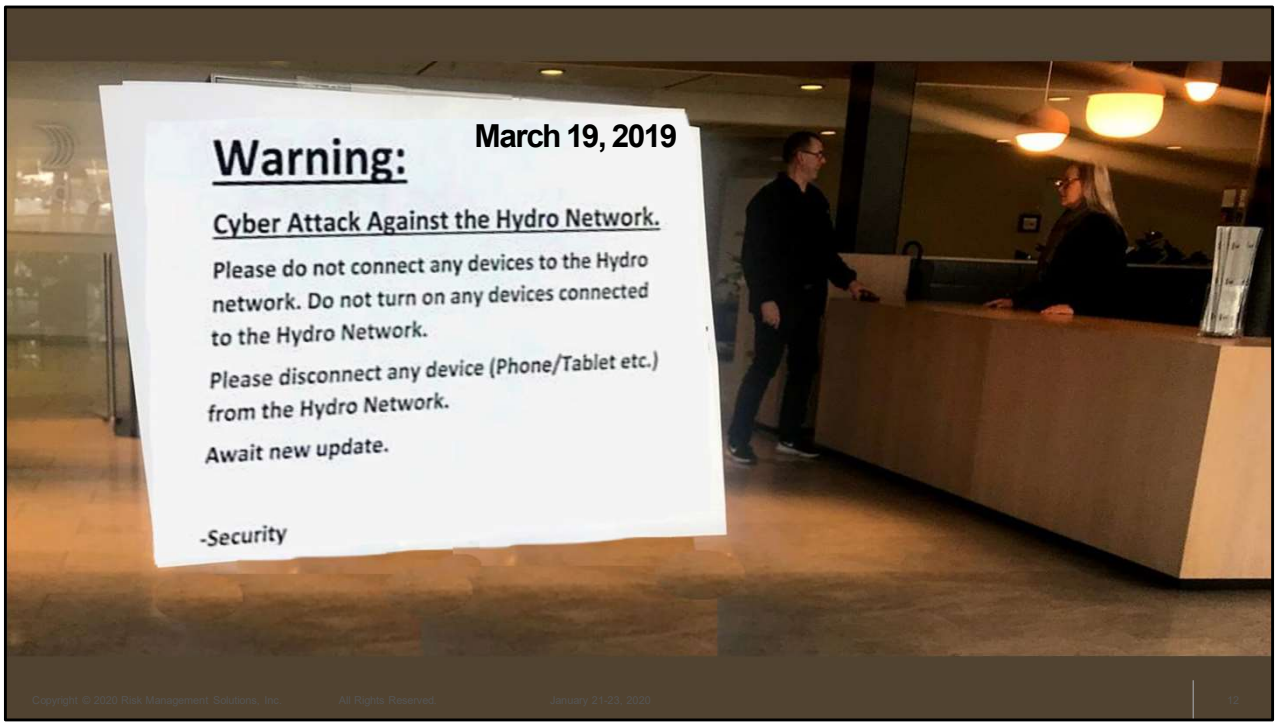


Now let's move on to the case study.

Norks Hydro is the world's seventh largest aluminum producer.
It is fourth largest outside of China.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

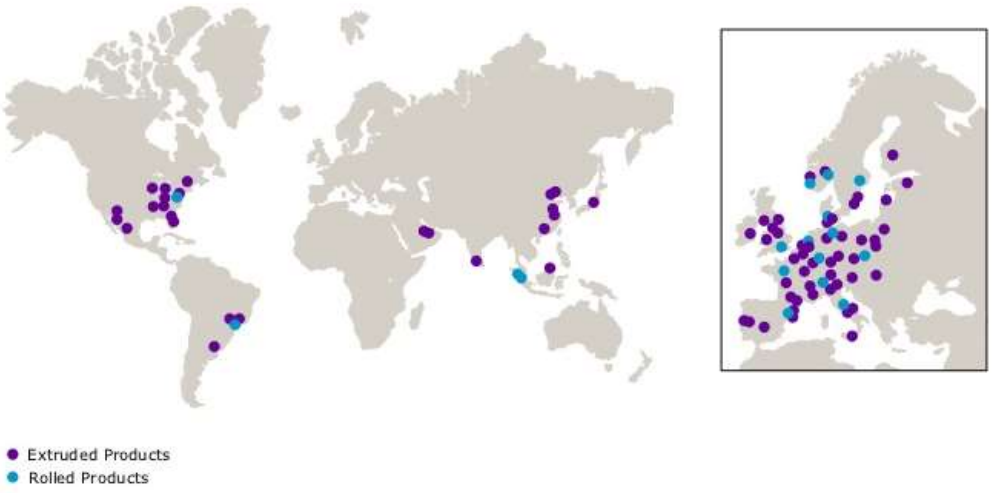
On March 19th of last year…



Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

…Norsk Hydro was victim of a worldwide ransomware cyber attack

Aluminium downstream worldwide network



Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

The attack mostly affected their Extruded Products operations, shown here in purple dots.

This attack made big headlines because – OH MY GOSH – RANSOMWARE HITS INDUSTRIAL CONTROLS!!!

NORSK HYDRO RANSOMWARE – HOW?

- Targeted Attack
- Threat Actor: "FIN6" Russian cybercrime group
- Initial compromise
  - Phishing (probably)
- Manual Lateral movement
  - Active Directory, etc.
- Malware distribution
  - SMB, …

- **Infected only Microsoft Windows**
- **No Industrial Control Systems were affected**

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

In fact, the ransomware attack only affected Windows systems and did not affect any industrial control systems. Even so, it was big and costly.

It's also important to distinguish this attack from the infamous NotPetya and WannaCry attacks, which were both contagious malware that spread automatically. Their victims were not necessarily targeted by attackers.

In contrast, this and similar attacks were definitely **targeted attacks.**

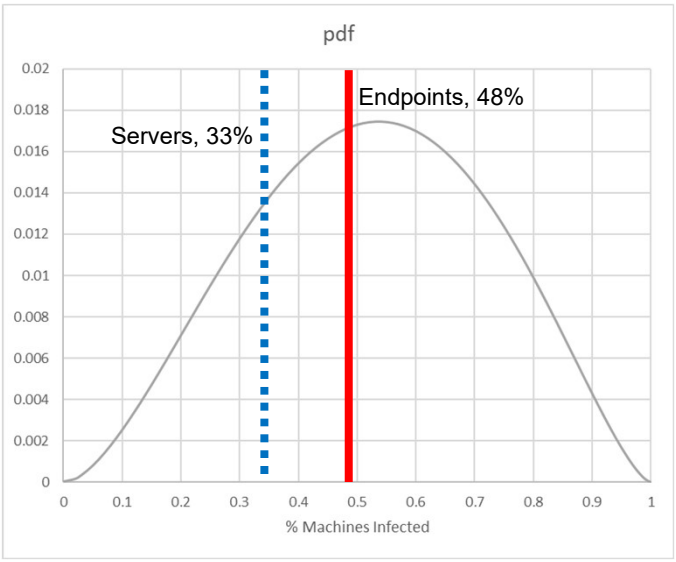
SCALE OF IMPACT

- Out of 23,000 PCs
  - 11,000 infected (**48%**)
  - 2,700 encrypted (**12%**)
- Out of 3,000 servers
  - 1,100 infected (**33%**)
  - 500 encrypted (**17%**)

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

In terms of scale of impact, it was pretty severe – 48% of end-user PCs and 33% of servers infected, with about 15% of each encrypted by the ransomware.

NORSK HYDRO **ACTUAL** INFECTION RATE VS. RMS **MODEL** FOR CONTAGIOUS MALWARE



Even though NOT CONTAGIOUS, infection rate in this case is ***fairly typical***.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Inside of RMS's model of contagious malware, we have a model component that is our estimate of the probability of "infection rate", ranging from 0% to 100%, with the mean of about 55%.

The two lines show the actual infection rate for Norsk Hydro. Seen through RMS's model, we would evaluate this result as "fairly typical" or "expected" if it **WAS** contagious malware, which it's not.

The message here is that a determined targeted attacker can achieve high infection rate even without automated propagation techniques.

REPORTED FINANCIAL IMPACT (EST)

- Q1: NOK 300-350 million
- Q2: NOK 250-300 million

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Here is the reported financial impact, in Norwegian Krone

Now you might be like David Puddy from *Seinfeld*, and you are comfortable counting in Norwegian Krone.

I think most of us are like Elaine.

REPORTED FINANCIAL IMPACT (EST)

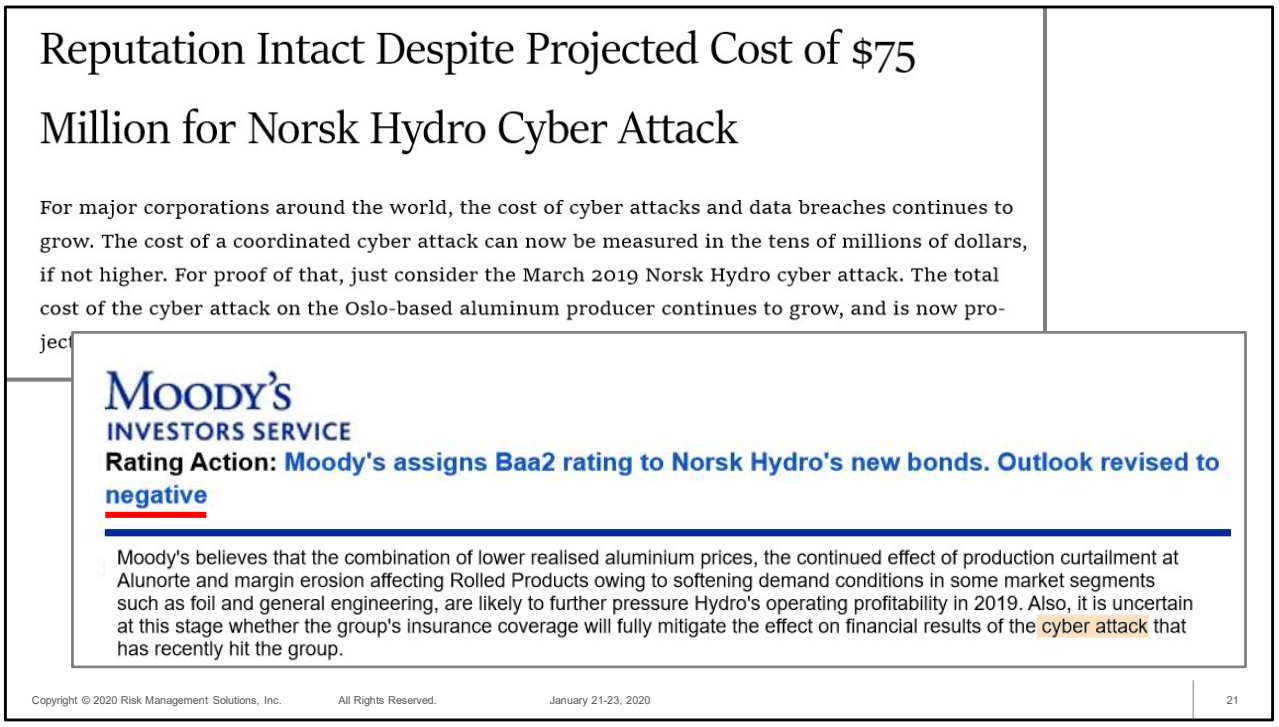
- Q1: $34.9 - $40.7 million
- Q2: $29.1 - $34.9 million

- Total: $64.0 – $75.6 million

8.6 kr = $1

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

We are more comfortable in US dollars. The reported costs are less startling, but still significant.



There was no evidence of broader business impact – lost customers, fines or other regulatory action.

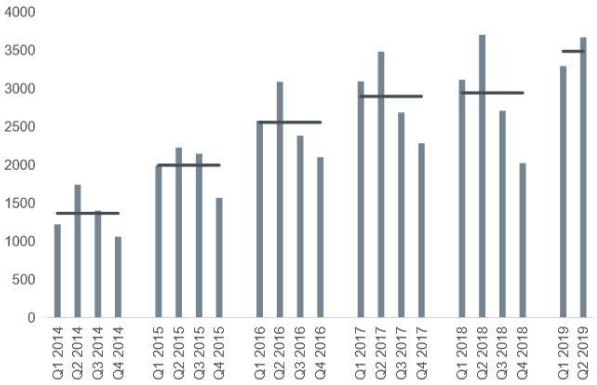
<click>

Right after the breach, Moody's Investor Service continued to rate Norsk Hydro as "medium grade" with "moderate credit risk", but with **negative** outlook.
The report mentions the cyber attack, but only regarding uncertainty of insurance payments.

Extruded Solutions earnings drivers

Hydro

Underlying EBITDA per tonne[1], NOK



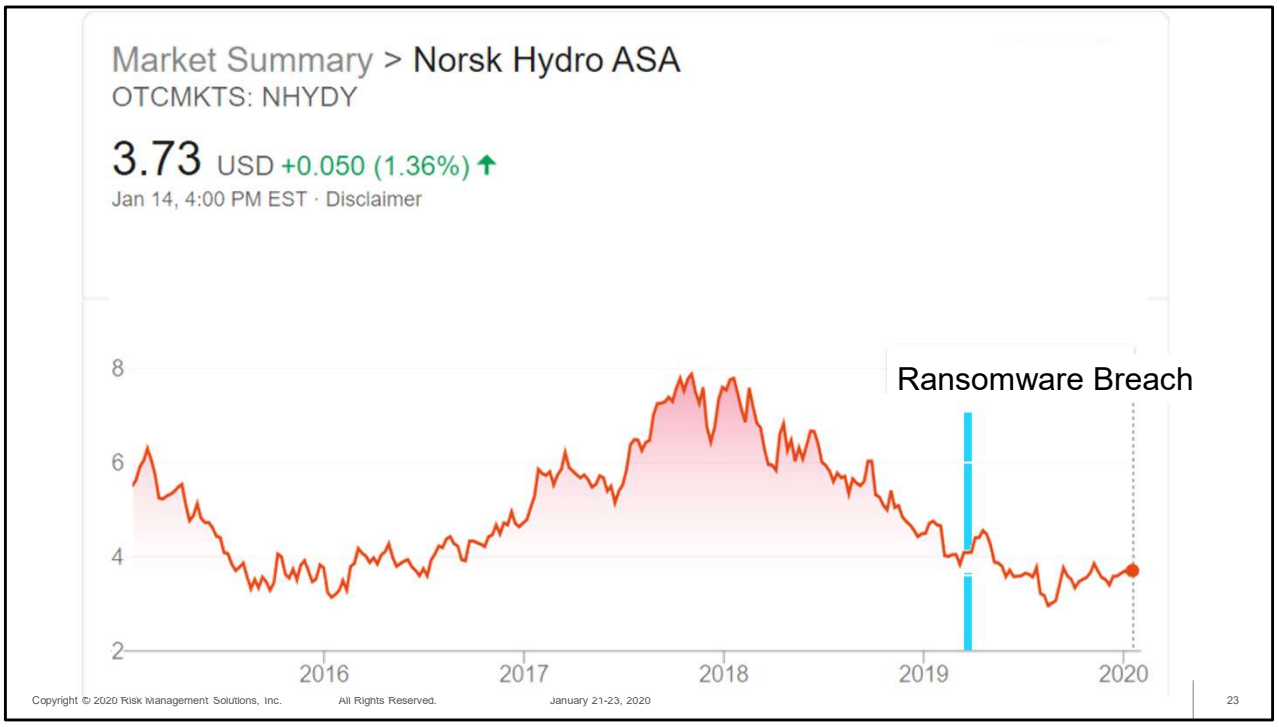
- Extruded Solutions aims to deliver minimum 10% average annual underlying EBIT growth over the next three years[2]
- Contract structure
  - Margin business based on conversion price
    - LME element passed on to customers
  - Mostly short-term contract, typically ranging from spot to 12 months, few longer term contracts with floating price or hedging in place
- High share of variable costs – high level of flexibility
- Annual seasonality driven by maintenance and customer activity
  - Stronger Q1 and Q2, weaker Q3 and Q4
- Strong focus on increasing value add to customers
- Preferred supplier market position in high-end products

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Let's put these costs in perspective.

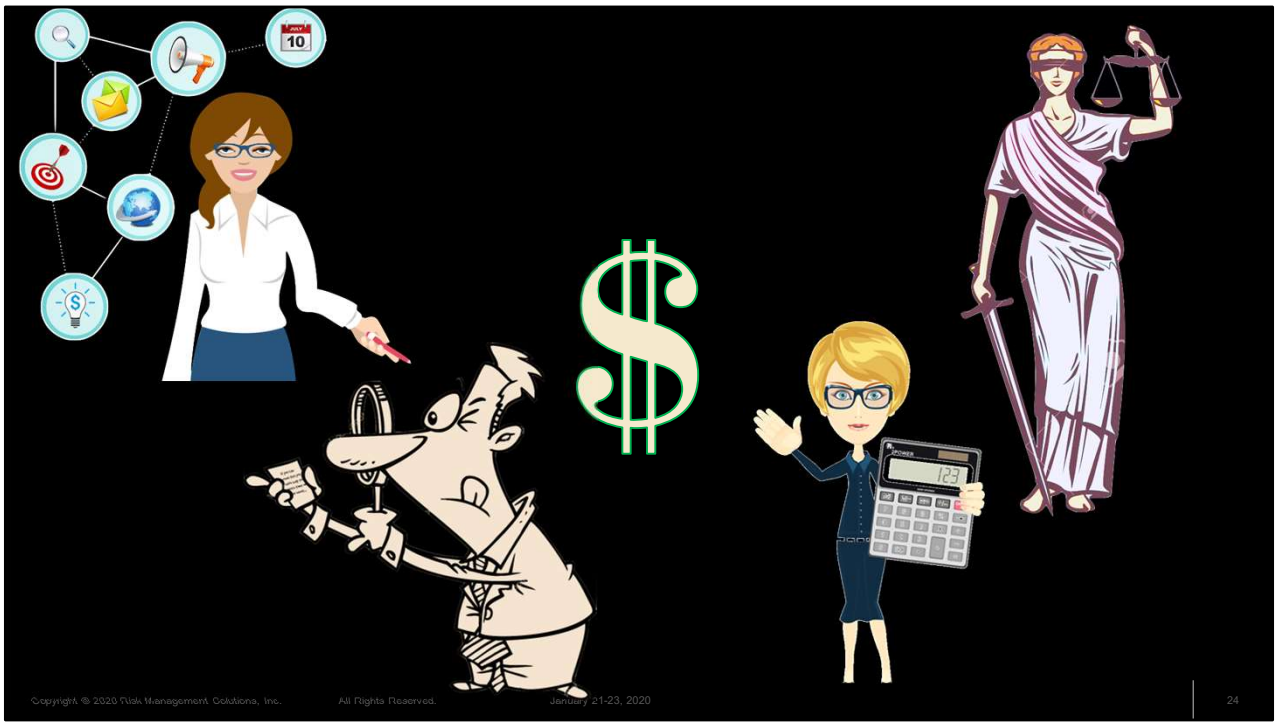
Norsk Hydro is a pretty complicated business with many different factors driving its performance. This slide shows just the Extruded Solutions business.

Compared to the cost of the ransomware attack, these drivers are much more significant and volatile.



Here's the 5-year chart of stock price.

Notice stock rallied a bit after the breach, but it didn't affect the overall trend which is dominated by other factors in the business and marketplace.



Before we move further, I need to make a very important point.

As engineers and technical experts, you may think that a counting money is simple – "a dollar is a dollar is a dollar…"

But in modern finance, there is no definition of "total cost of a data breach" that would serve all purposes.

<click>

There is the perspective of CAPITAL INVESTMENTS, which supports investment decisions using return on investment.

<click>

There is the perspective of FINANCIAL ACCOUNTING, for both financial statements and taxes.

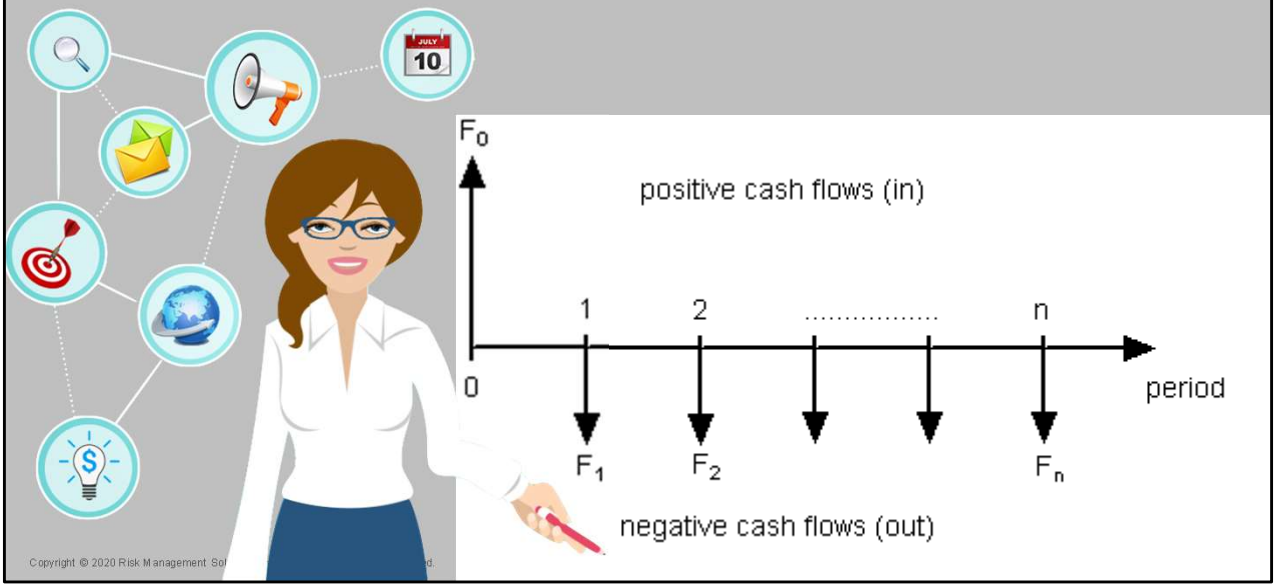
<click>

There is the perspective LAWS and REGULATIONS, including cost recovery, fines, and lawsuits

<click>

Finally there is the perspective of INSURANCE, which has its own rules for what is included or excluded from a loss calculation

1) Think Cash Flows



This leads to my first main message:

If you are responsible for managing cyber security in an operating company, you need think of money like an INVESTMENT ANALYST would – which is discounted cash flows.

Modern ROI analysis for investment decision support

DISCOUNTED CASH FLOW ANALYSIS

- Forward looking ("ex ante")
- Everything is an (uncertain) cash flow
  - No non-cash charges like depreciation, goodwill, etc.
- Discount all cashflows by your cost of capital (~business riskiness)
  - A dollar today is worth more than a dollar next year
  - A sure-thing dollar is worth more than an uncertain dollar

- DON'T EVER COMBINE FORWARD AND BACKWARD ANALYSIS!

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

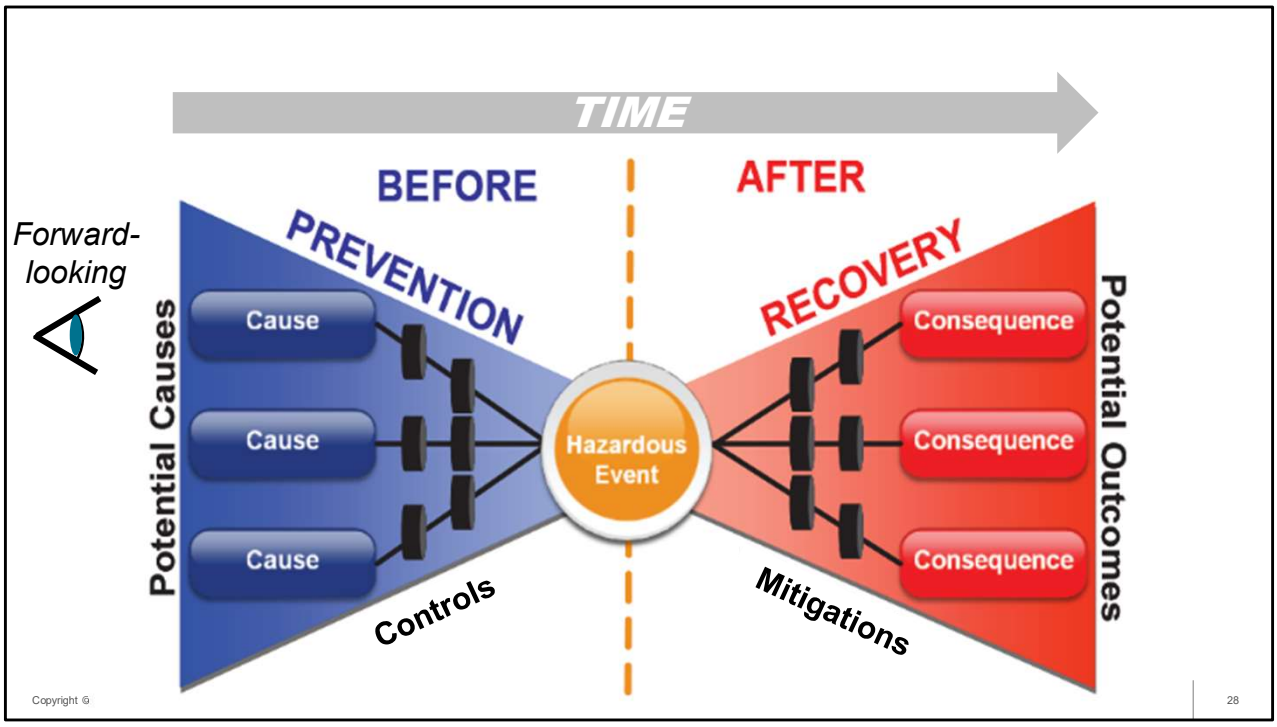
I can't cover this in detail today, but there are plenty of good books that explain discounted cash flow analysis.

There are three points I want to emphasize:

1) Always forward looking!
2) Insurance payments often come many months or years after the loss event, and they are uncertain. Therefore they count less than a dollar in hand today.
   - Best way to do that is to prevent or quickly mitigate the breach cost.
3) Never combine forward and backward analysis. It's apples plus oranges. Creates a mess.

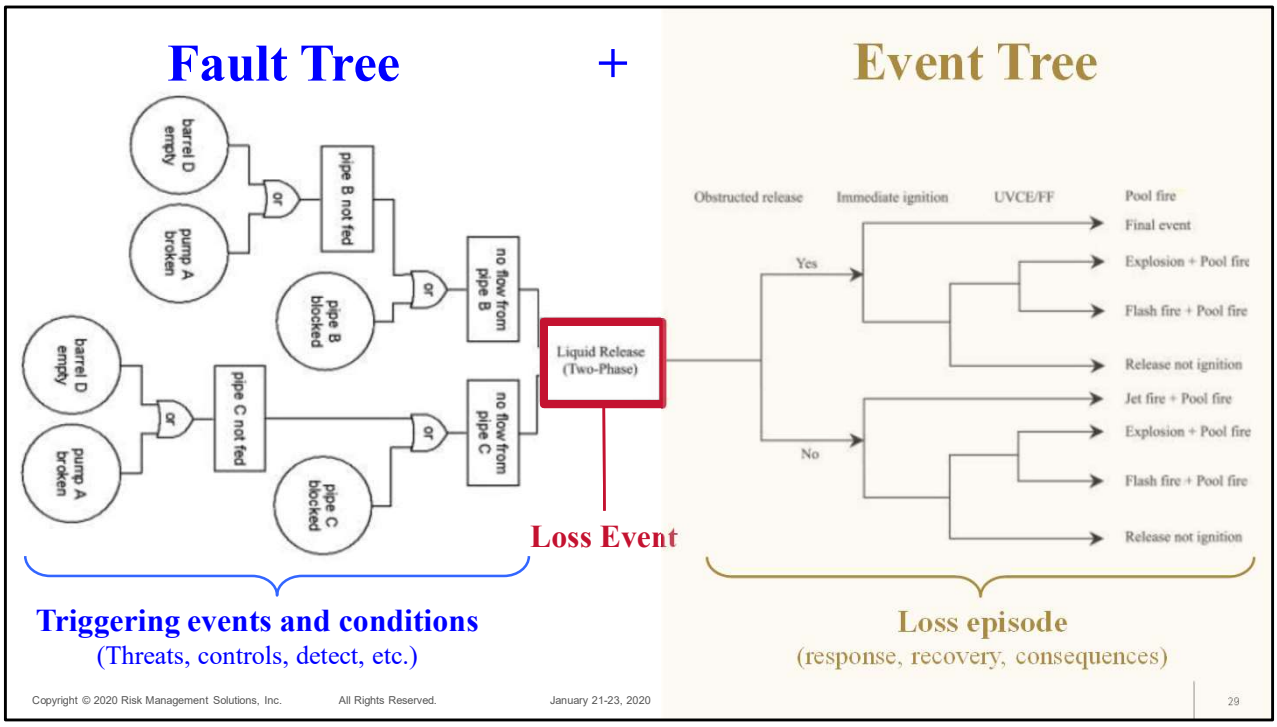
2) Think Bow Ties

This leads to my second main message.



By “bow ties”, I mean a “bow tie” model of a loss event, with the causal processes on the left side and the cost or loss processes on the right side.

The “eyeball” icon here is to remind you what “forward looking” means.

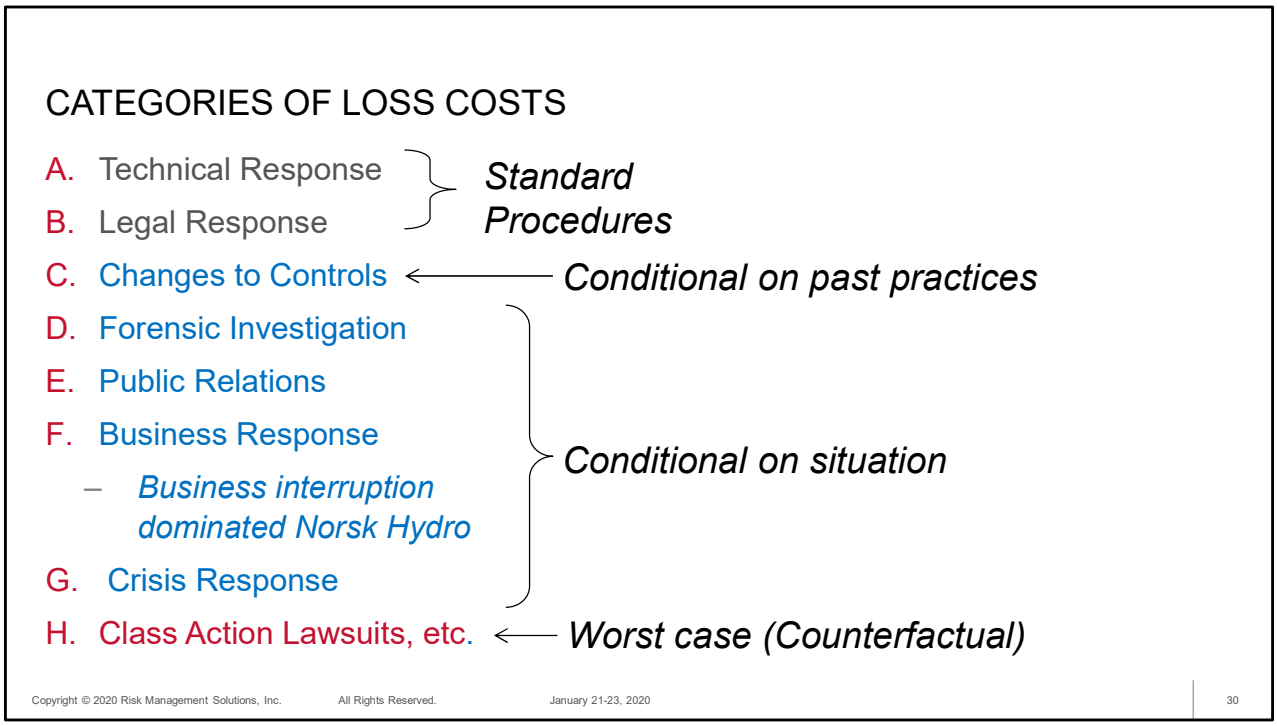


Here is a more specific version.

Many of you have training in reliability engineering, and you'll be familiar with event tree analysis. The nodes are probabilistic states and the connectors are logic blocks – AND, OR, and NOT. That's the left side.

The right side is a probabilistic event tree – or more specifically a Branching Activity Tree. The loss event triggers some activities, and then with a probability these spawn new activities.

Most quant. risk methods, including FAIR, are just specific ontologies to help you build a probabilistic model like this, factoring in the effectiveness of controls.



For today, we are just going to look at the right side – the loss processes

Here are eight general categories of costs. Let's consider what drives them in terms of probability.

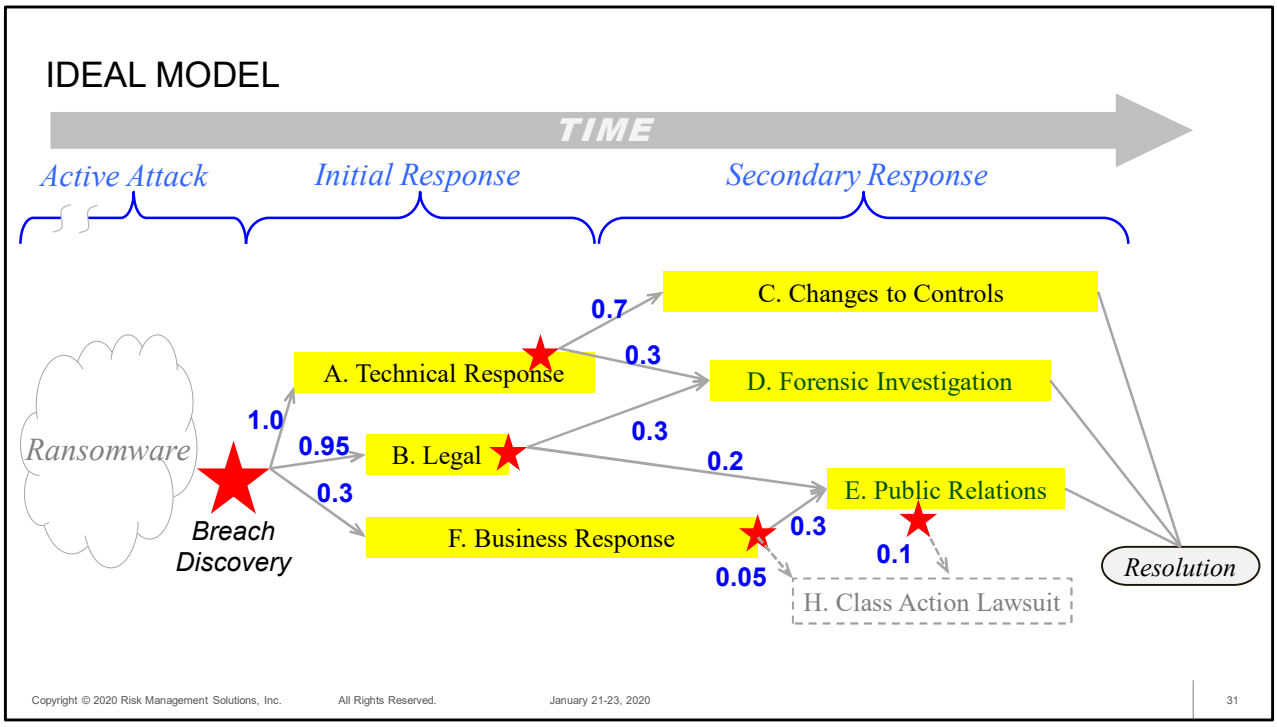
The first two are usually driven by standard procedures, unless something nasty is discovered or you get sued.

Category C depends on if you have a lot of "security debt" built up, or not. You see this in the news frequently about major breaches.

Categories D through G are totally conditional on the situation – the nature of the breach, the threat actor, how the loss events are handled, etc.

Norsk Hydro did a particularly good job with Business Response – recovery and continuity, and also crisis response, including public communication.

This is why they avoided the worst-case costs – Category H. Contrast this with Equifax and other notorious cases.



So how would you model breach impact using a branching activity model. Here is an idealize model

This diagram is something like a Gantt chart. The length of each bar is how long it takes. The cost for most processes is the length of time multiplied by the resource cost per unit time. Usually it isn't too hard to estimate a probability distribution for each process, given the severity of the breach.

The stars here mark branching points, where one process might spawn another. The blue numbers are the branching probability.

Accepted for *12th Workshop on the Economics of Information Security*
version 2.0

How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches

Russell Cameron Thomas
Department of Computational Social Science, George Mason University, Fairfax, VA 22030, russell.thomas@meritology.com

Marcin Antkiewicz
Qualys, Inc., Madison, Wi, 53704, mantkiewicz@qualys.com

Patrick Florer
Risk Centric Security, Inc., Dallas, Texas 75230, patrick@riskcentricsecurity.com

Suzanne Widup
Verizon RISK Team, Verizon Communications Inc., San Francisco, CA 94105, suzanne.widup@verizon.com

Matthew Woodyard
Zions Bancorporation, Salt Lake City, UT 84133, mwoodyard@5lbs.org

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

This paper gives you all the details if you are interested

Status update cyber attack

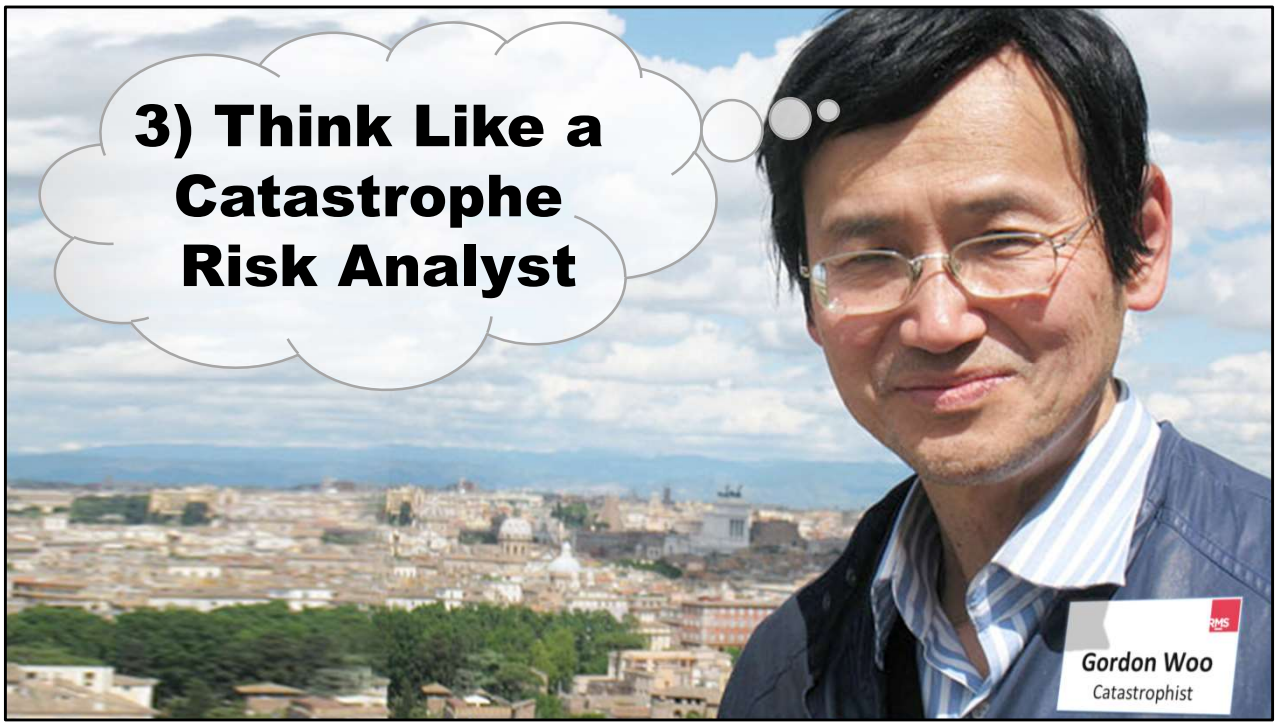
Operational and financial impact

- Overall financial impact for Q2 NOK 250-300 million
  - Of which Extruded Solutions NOK 150-200 million
- Overall financial impact for Q1 NOK 300-350 million
  - Of which Extruded Solutions NOK 250-300 million
- At end-Q2 operations have largely returned to normal
- Limited financial impact estimated for Q3 2019
- Hydro has a robust cyber insurance policy in place with recognized insurers

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

So what did Hydro tell us about breach costs.

Almost nothing, other than to say that “business interruption” was the biggest cost.

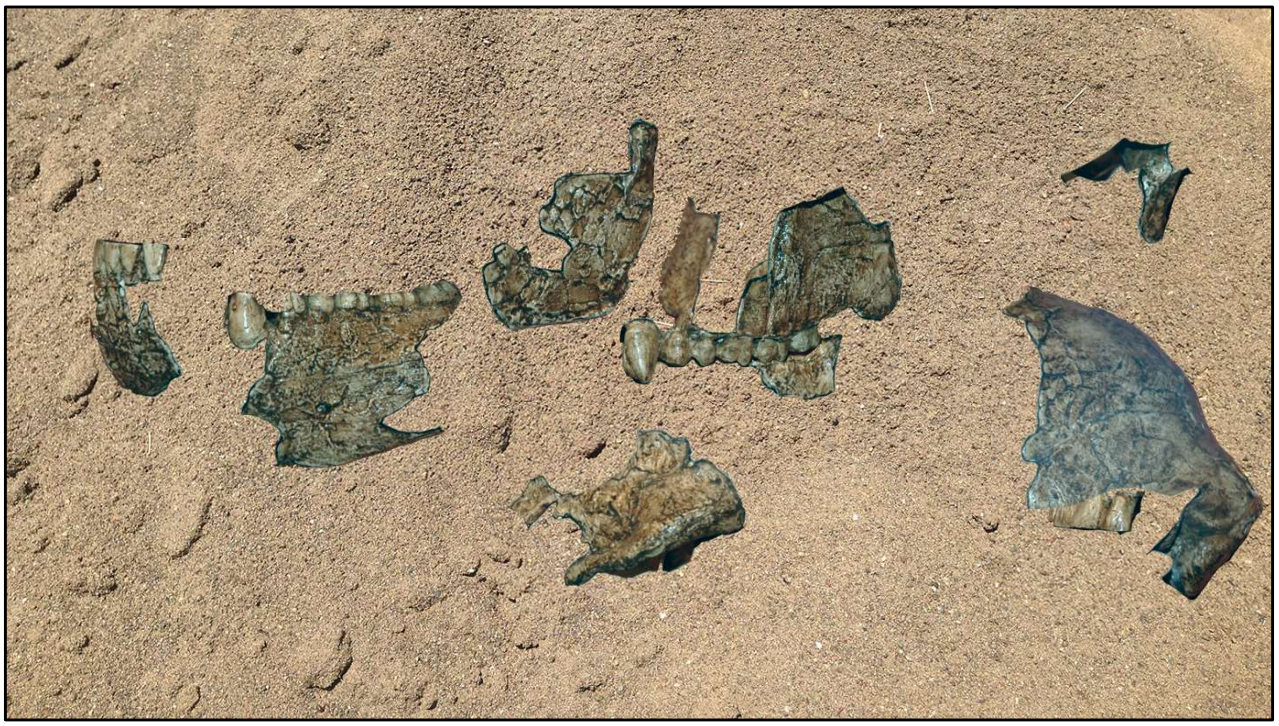


That brings me to my third main message.

This is my colleage at RMS – Gordon Woo – whose actual title is “Catastrophist”. Isn’t that cool?

The word “catastrophe” here doesn’t mean “Doomsday Scenario”. Instead it means “worse than ordinary”, like 50-year flood, 100-year flood, and 1,000-year flood.

By “risk analyst” I don’t mean to imply some mathematical Nirvana where we are floating in pure clean data.

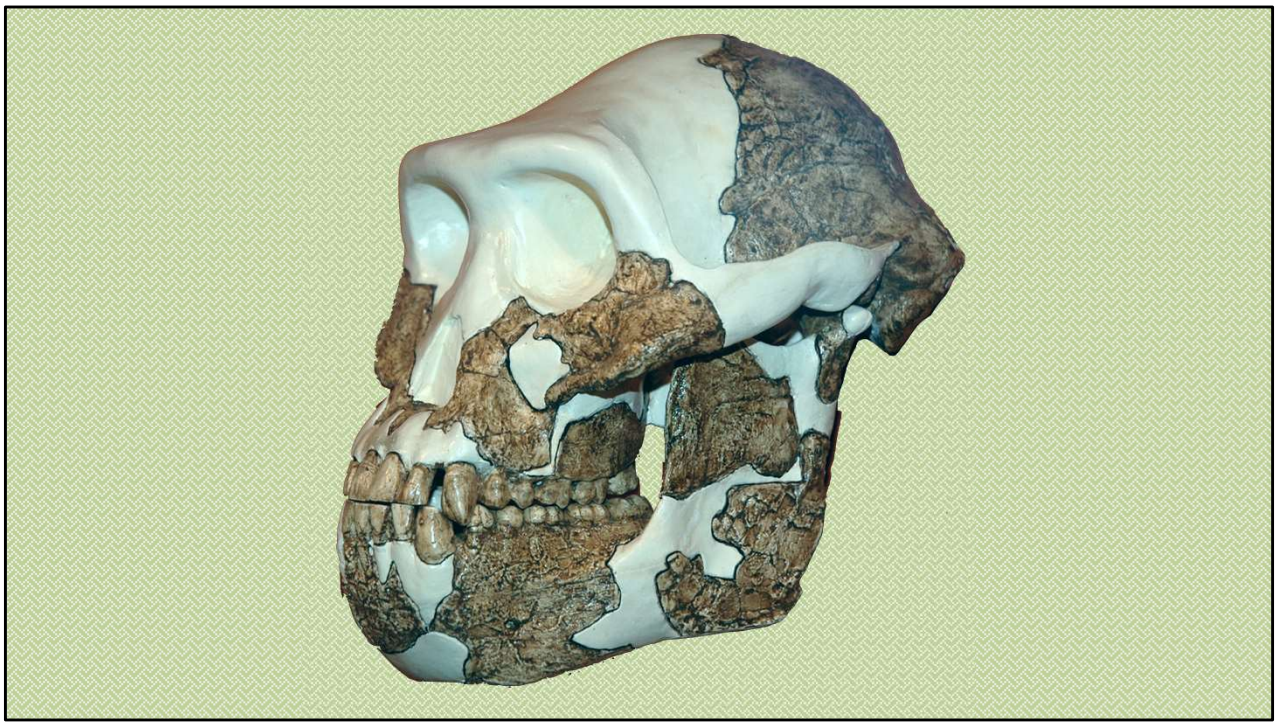


Instead, it’s more like this – Paleontology.

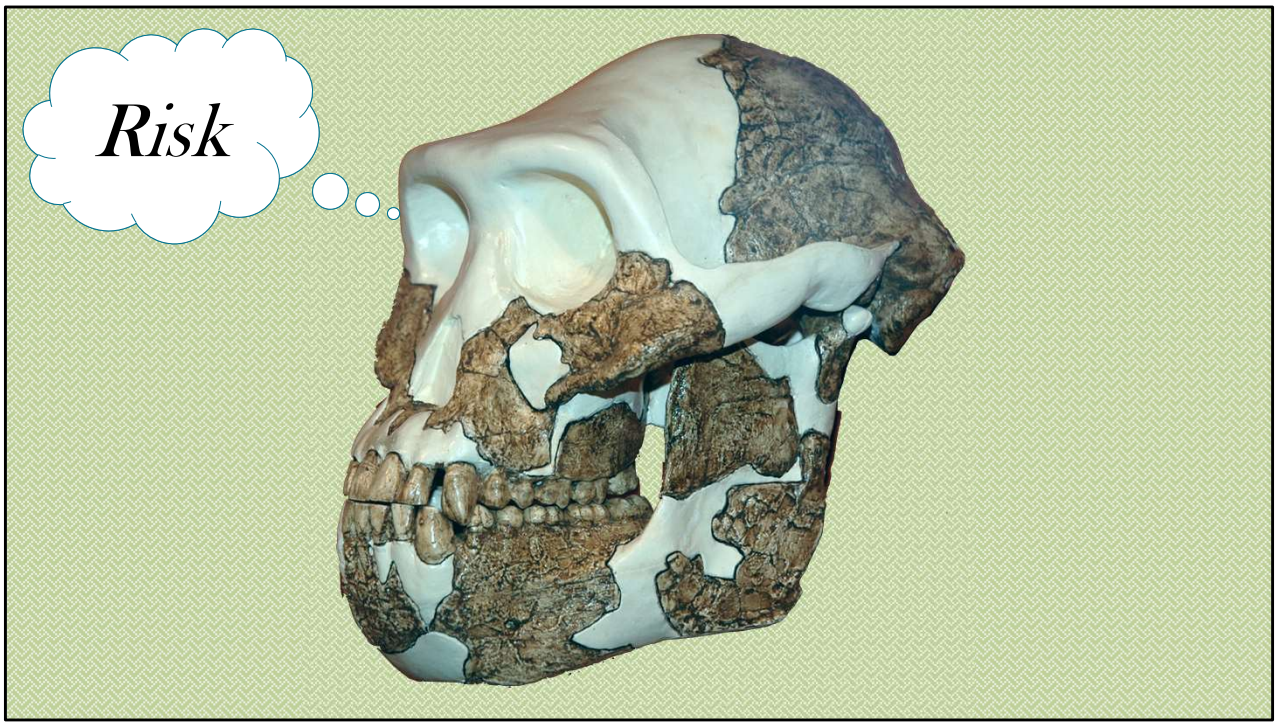
At first, everything looks messy and maybe worthless.

But then you isolate the key elements

Figure out how they fit together



Fill in the missing pieces with some reasonable inferences and available theory



And – *voila* – you come out with a reasonable model of risk

In other words – we can't and don't depend on having an "actuarially adequate" database of loss events, like they do in life insurance.

Instead, we collect a wide range of evidence, identify causal mechanisms and probabilistic relationships, accounting for uncertainty, and grounded where possible in theory.

DIRECT EVIDENCE

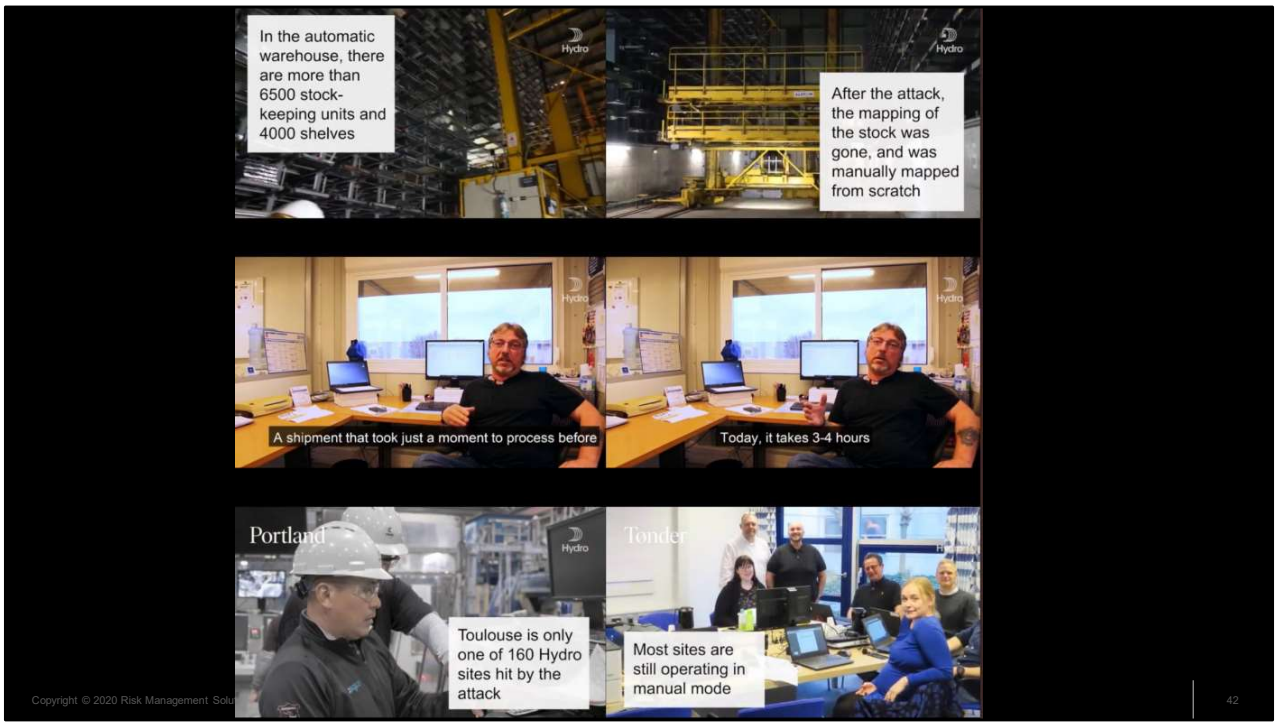
- PLENTY of evidence:
  - Business interruption
  - Business and IT recovery costs
- NO evidence:
  - External law firm or legal costs
  - External PR
  - Regulatory activity or costs
  - Loss of market share, pricing power, etc.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Back to the Norsk Hydro case, and specifically just the public information.

We see positive evidence for BI costs and business + IT recovery costs.

But there is also an absence of evidence for other costs we might expect for a breach of this magnitude. Usually there would be some observable indicators for each of these.



Though it's PR activities, Hydro shared plenty of anecdotal information about recovery processes that were clearly costly.

MANUAL EFFORT WITH EXISTING RESOURCES

– In Belgium, a long-time sales manager printed out the entire order book for Hydro's welded tubes plant, just hours before the cyber-attack had been identified. This print of orders created the foundation for a complete manual system at the Lichtervelde site.

– In Germany, where usage of the SAP system was limited, the 10-person material management team in Hamburg found that their emergency plan was a life-saver for the rolled products site. Especially the lists of their 16,000 spare parts – which they had printed out months ago.

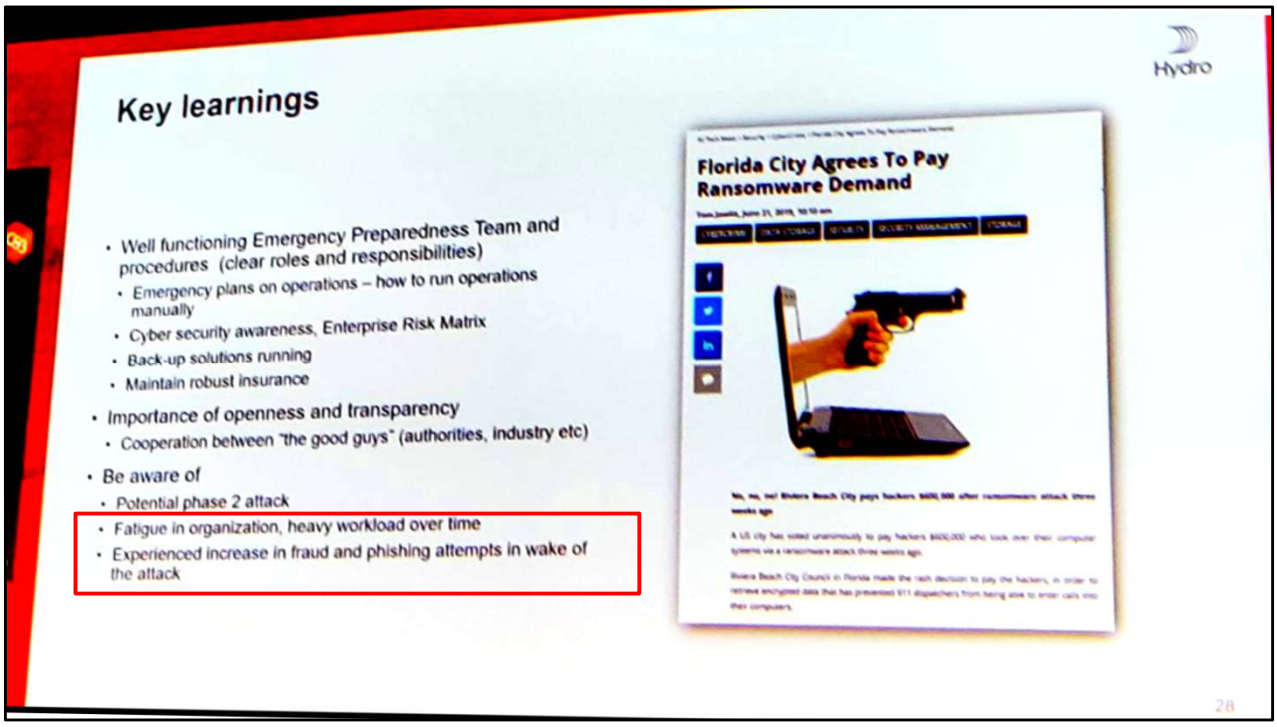
– In France, four marketing colleagues traveled from Paris to Rennes, then to Nantes and down to Toulouse, to scan and retrieve PCs at each site. The 1,300-kilometer trek enabled IT teams to handle emergency issues in their building systems business.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Take note of these manual efforts, especially the two highlighted.

I'm willing to bet that the cost of "printing out the entire order book" and the "one thousand three hundred kilometer trek" were not included in Hydro's cyber attack cost as it appears on their financial statement. Likewise, probably not included in losses for insurance purposes.

Why? Because these were costs incurred by their existing staff and resources (printers, paper). (We'll come back to this.)



Here is some more evidence related to the cost of recovery. This is a slide Hydro presented at a conference, posted on Twitter.

Notice the two items at the bottom – 1) organization fatigue and 2) increase in fraud and phishing attempts after the attack

COMPARABLE CASES

Same threat actor, same tools and techniques, same timeframe

Victim	Cyber Insurance?	Gross Cost	Pay?	BI?	3rd Party Tech Svs.	External PR	Compli-cations?
Norsk Hydro (Aluminum)	Yes (*$3.8M*)	$64M – $75.6M	No	Yes	No	No	Yes
Altran (Eng. Consulting)	Yes (*$2.7M*)	$17M	No	Yes	Yes	No	No
Hexion (Plastics)	Yes ($5M)	$13M	??	No	No	No	Yes
Momentive (Chemicals)	??	??	??	??	??	No	??
Nyrstar (Metals)	??	??	??	No?	??	No	YES

(*partial payment*)

(Exec. turnover, lawsuits, regulator actions)

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

What other evidence do we have.

One very valuable category is evidence from comparable cases. In addition to Norsk Hydro, we know of four other industrial companies targeted by the same group, using the same tools and methods, in the same campaign.

We can compare the reported cyber insurance payouts. In two cases, they are partial payments, but these are probably half or more of the final payout.

Not all firms experienced business interruption, and apparently only one firm paid for external tech. services – forensics and so on.

None paid for an external PR firm.

This last column – "Complications" – deserves some attention.

4) Fragility Matters

This brings us to the fourth main message. When it comes to business impact, fragility of the business matters.

COMPLICATIONS

- Norsk Hydro (pre-)
  - **Executive void** – CEO early retirement. CFO had to stand in. share price down by 40 percent in the prior 13 months
  - **Legal sanctions** – Court-ordered shutdown of parts of its Brazilian operation due to a toxic spill from one of its plants. Stock price down ~40%.
- Hexion (post-)
  - **Chapter 11 bankruptcy filling**
    - Excessive debt to fund acquisitions
- Nyrstart (post-)
  - Shareholders **wiped out** in take-over by supplier
  - Accountants "**unable to certify**" financial statements, etc. Shareholder lawsuits.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

In the case of Hydro, the complications came just prior to the breach. Remember the stock price chart? Given this context, it's remarkable that Hydro managed the response and recovery as well as they did. It could easily have been much worse.

In the cases of Hexion and Nyrstart, their complications came post-breach, and were unrelated. Both were in major financial trouble. In the case of Nyrstart, there is a possibility that the ransomware attack caused the loss of some important documents and communications, contributing to their accountant's negative report.

The message here: If your business is already fragile, the cost and consequences of a given cyber attack could be much, much worse than normal.

THREAT ACTOR: “FIN6” RUSSIAN CYBERCRIME GROUP

- Operating since 2015
- Primary method of operation
  - Stealing payment card details by compromising point-of-sale (PoS) systems in Hospitality and Retail
- Recent activity
  - LockerGoga and Ryuk ransomware to compromise POS systems
  - LockerGoga ransomware to attack industrial companies

No previous ICS attack capabilities
No known collaboration with state-sponsored attack groups

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

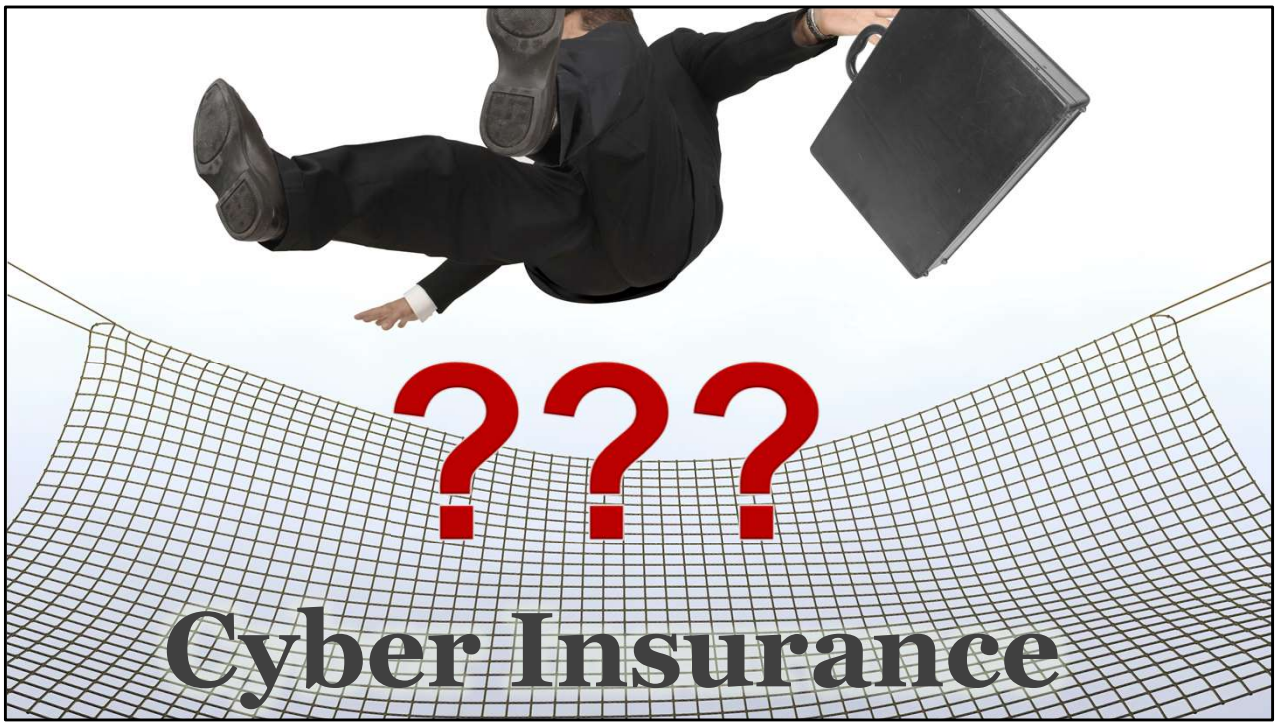
The last class of evidence regards the threat actor.

In this case, it has been attributed to the FIN6 Russian cybercrime group.

What’s important to note about this group is that they only recently started attacking industrial firms. Apparently, they have no previous experience or capabilities for attacking industrial control systems.

It appears that this campaign is attempting to find another “soft target group” that will pay ransoms – much like health care organizations and local governments in the US.

To build out a probabilistic model, we need to estimate the likelihood and impact of counter-factuals like threat actors with more ICS experience and capabilities, or threat actors with different motives, such as state actors.



Now, in the time remaining, let's shift to cyber insurance.

5) Cheese with holes can still be good

Copyright © 202

The main message here is that “Cheese with holes can still be good cheese”

WHAT WE KNOW ABOUT HYDRO'S CYBER INSURANCE COVERAGE

(this page is intentionally* left blank)

*AIG is primary carrier

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Unfortunately, we know almost nothing about Hydro's cyber insurance other than they have some and AIG is the primary carrier.

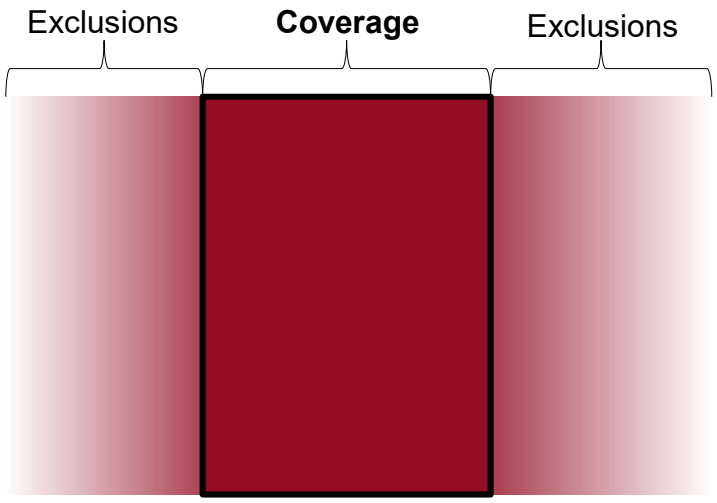
So my points here are generic and will hopefully help you understand cyber insurance better and how to work with the insurance people at your firm.

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

First – Cyber insurance is not simple – any more than “industrial control systems” is just about on-off switches.

I’m going to give you a flavor of some of the complexities.

GROUND-UP LOSS



Area = $ G.U. Loss

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

The total amount of the loss, exclusive of any insurance coverage, is called “ground-up loss”. In this diagram, the area of the red rectangle is proportional to the ground-up loss.

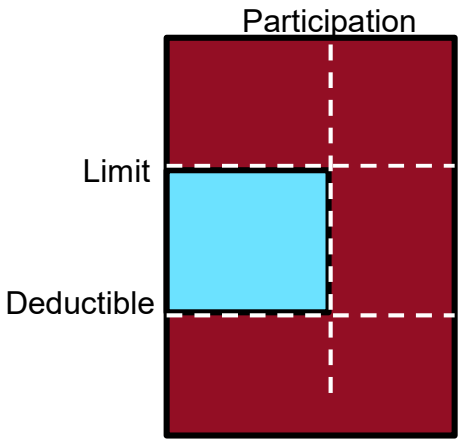
But as I have already mentioned, there will be many “real” costs that are excluded for one reason or another.

If you've ever read a business insurance contract, you might feel like you are in a Marx Brother's routine:

"The party of the first part shall be known in this contract as the party of the first part."

Goes without saying: contracts are written for lawyers, not people like you and me.

PRIMARY COVERAGE



"Affirmative"?:
- Yes = "cyber insurance"
- No = bundled in property or liability insurance *(> 90% of market)*

Other possible limits:
- Site-level
- Policy-level
- Geography
- Jurisdiction
- Annual frequency

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Here's what that looks like schematically.

Every insurance policy will have limits – a deductable or attachment point, an upper limit, and a participation percentage.

<click>

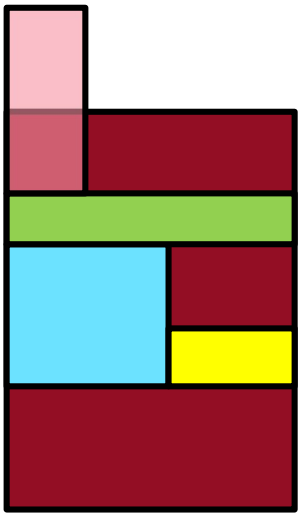
There are other types of limits possible, including per site, per policy, per geography or jurisdiction, and per yer

<click>

Further complicating things is whether it is an affirmatively a cyber insurance policy or bundled.

The legal battle over Merck and NotPetya ransomware involves bundled, non-affirmative cyber insurance.

FULL CYBER INSURANCE "TOWER"

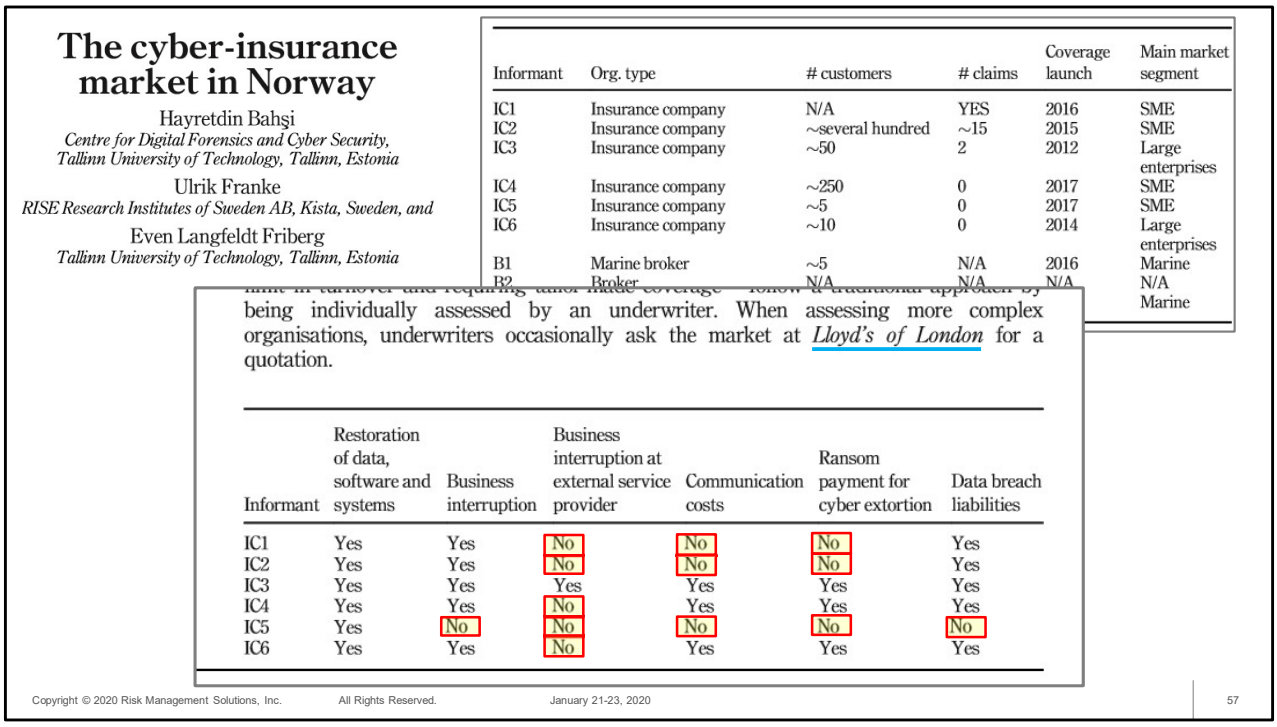


Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

So for most large companies and organizations, what you'd end up with is a "tower" of insurance from different carriers, each with different limits and terms.

You end up with "Swiss cheese" – coverage in some scenarios but not in others.

The basic reason for this is the interests of insurance companies – diversification, solvency, finance, regulations – are different from the interests of the insured – YOU.



The cyber-insurance market in Norway

Hayretdin Bahşi
Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Tallinn, Estonia
Ulrik Franke
RISE Research Institutes of Sweden AB, Kista, Sweden, and
Even Langfeldt Friberg
Tallinn University of Technology, Tallinn, Estonia

Informant	Org. type	# customers	# claims	Coverage launch	Main market segment
IC1	Insurance company	N/A	YES	2016	SME
IC2	Insurance company	~several hundred	~15	2015	SME
IC3	Insurance company	~50	2	2012	Large enterprises
IC4	Insurance company	~250	0	2017	SME
IC5	Insurance company	~5	0	2017	SME
IC6	Insurance company	~10	0	2014	Large enterprises
B1	Marine broker	~5	N/A	2016	Marine
B2	Broker	N/A	N/A	N/A	N/A

being individually assessed by an underwriter. When assessing more complex organisations, underwriters occasionally ask the market at *Lloyd's of London* for a quotation.

Informant	Restoration of data, software and systems	Business interruption	Business interruption at external service provider	Communication costs	Ransom payment for cyber extortion	Data breach liabilities
IC1	Yes	Yes	No	No	No	Yes
IC2	Yes	Yes	No	No	No	Yes
IC3	Yes	Yes	Yes	Yes	Yes	Yes
IC4	Yes	Yes	No	Yes	Yes	Yes
IC5	Yes	No	No	No	No	No
IC6	Yes	Yes	No	Yes	Yes	Yes

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

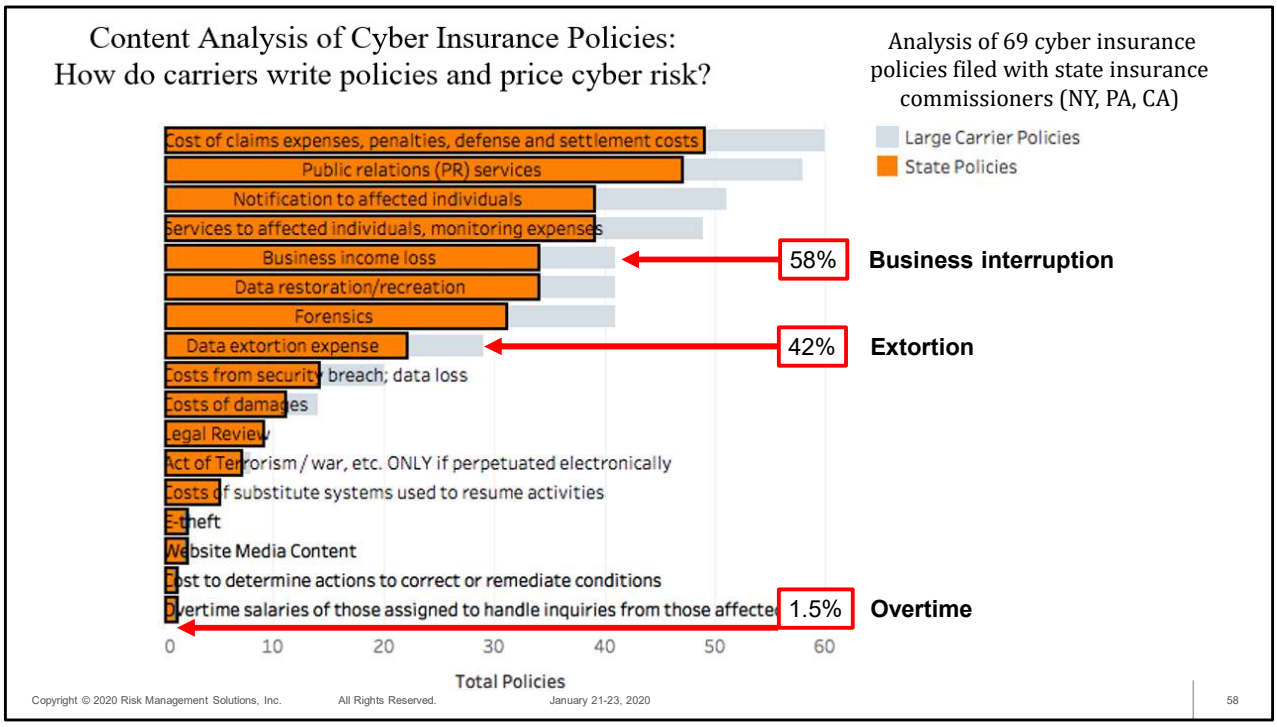
To fill out the picture, here are some findings from academic papers.

First is a study of some insurance companies in Norway.

Norks Hydro gets primary coverage from AIG, one of the largest insurance firms in the world, and so these findings only serve as a background

<click>

Looking at policies from six firms, notice the variability in what is covered and what isn't. Only one covers the cost of business interruption at your external service provider (e.g. cloud services).



Here's another study, this time of about 70 polices filed with regulators in three US states.

<click>

This chart shows number of policies offering a class of coverage

<click>

58% cover business interruption

<click>

42% cover extortion

<click>

But only one out of 69 – 1.5% -- cover overtime salary costs such as what Norsk Hydro experienced

What do we know about cyber risk and cyber risk insurance?

Martin Eling and Werner Schnell
University of St. Gallen, St. Gallen, Switzerland

Literature review of 209 papers

Findings – The results illustrate the immense difficulties to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of change and incalculable accumulation risks. The authors discuss various ways to overcome these insurability limitations, such as mandatory reporting requirements, pooling of data or public–private partnerships in which the government covers parts of the risk.

institutional innovations

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

Finally, here is a literature review study of 209 academic papers.

<click for each point>
Overall, they find big problems in cyber insurance,
- due to lack of data and models,
- the uncertainties due to face pace of change, and
- so-called “accumulation risks” – in other words, how bad could a single insurance company get hit if many of their customers have losses at the same time.

The proposed remedies all involve institutional innovations – which by the way is the topic of by PhD dissertation.

Closing the cyber insurance discussion – you may have been told that cyber insurance is a way to **transfer** risk to the insurance company.

That's the wrong way to think about it.

Instead I want you to think of cyber insurance as another form of Risk Finance that can help your business survive a severe attack.

In this way, it's like your borrowing capacity, your ability to sell assets or sell equity, or any other way of paying for extra ordinary costs.

Thank You

russell.thomas@rms.com

@MrMeritology

Copyright © 2020 Risk Management Solutions, Inc. All Rights Reserved.

With that I will close and thank you for your attention.

Here's my email address and Twitter handle.