PRACTICAL CYBER – Pragmatic + Cutting-Edge = Greater Protection

SPECIAL HELP FOR HEALTH PLANS

IS YOUR HEALTH PLAN PREPARED TO HANDLE THE SIGNIFICANT FINANCIAL RISKS OF TODAY'S CYBER-ATTACKS?

THE PROBLEM: CYBER RISKS FOR HEALTH PLANS ARE BUSINESS THREATENING

A scary scenario to consider – total computing shut down for 9 days

Most health plans – indeed most businesses – don't fully understand the significant financial risks they face from today's cyber-attacks:

- Every health plan depends heavily on computing technology; and
- Cyber-attacks are becoming more prevalent, sophisticated, and faster – which decreases the time to react and increases the financial risks.

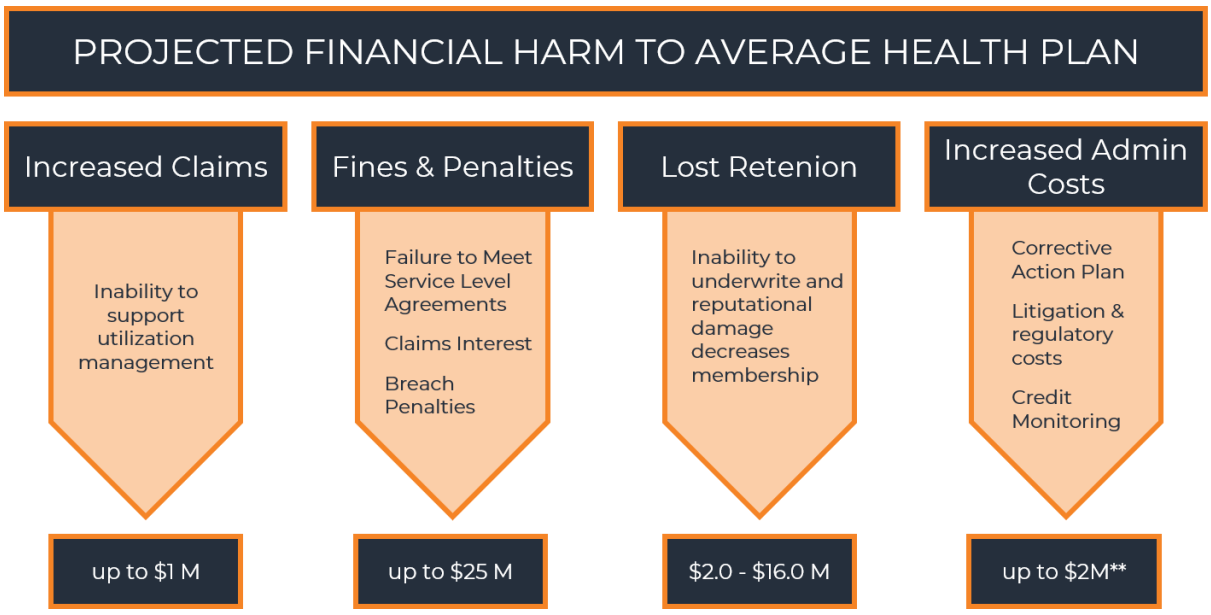
To appreciate the significance of your cyber risks, ask yourself what would happen if all your computing devices and systems were shut down for 9 days? Most likely, this would stop you from:

- Paying claims, collecting revenue, and paying bills
- Utilization management
- Collecting, reviewing, or sharing enrollment data
- Responding to member and provider inquiries
- Underwriting renewal or new business
- Ensuring your vendors have the information needed to support your business

For a glimpse into the ensuing financial harm, we created a financial model that produced the following estimates for a sample health plan with 250K members, average premium of $450 PMPM, operating at a 90% MLR with 2% margin that holds contracts with service level guarantees and penalties for failure. The model applied moderate impact assumptions that could be much worse. For example, lost retention reflects margin and contribution to fixed expenses. Health insurers often carry variable costs associated with staff and contracts that are not easily reduced even when there are significant membership

changes. Additionally, administrative costs would be much higher if the insurer experienced a Class Action suit like Anthem (see below for details).

cz



The underlying analysis is consistent with the modeling NAIC recommends insurers use to evaluate the stress a cyber-attack could place on performance and capital. In this scenario total impact is significantly driven by penalties existing in the contracts of our illustrative insurer. It is possible for an insurer to carry contractual risks that have not been fully analyzed through the current risk assessment process because it is not focused on financial harm. Ranges are impacted by the plan's preparedness to support key operations and reduce reputational harm in the event of a cyber-attack and the amount and quality of your insurance coverage.

If you doubt that a 9 day interruption of your computing systems is a realistic probability, think again. It is exactly what happen to Merck in June 2017 when it got hit by the NotPetya cyber-attack:

- On June 27, 2017, despite Merck having a dedicated, well-staffed internal cybersecurity team, the NotPetya cyber-attack infected tens of thousands of Merck's computers in 65 countries.
- In various public disclosures, Merck estimated the attack cost them about $915 million – stemming from the attack crippling in-house API manufacturing and hindering its R&D, other operations, and formulation and packaging systems;
- Merck reported the attack had a $260 million impact on sales, $330 million impact on marketing and administrative expenses and production costs, and a $200 million impact on 2018 sales through residual backlog.

Many other major companies fell victim to NotPetya – the international law firm DLA Piper (which has a sophisticated cybersecurity practice but did not announce a damage amount), Reckitt Benckiser (announced $136 million in damage), FedEx (announced $300 million in damage), the advertising group

WPP (announced $19.25 million in damage), and the shipping giant A.P. Moller-Maersk (announced $136 million in damage). All of these major companies had cybersecurity systems far more sophisticated than most health plans.

When it rains, it pours – Class Action Suits

Health plans have to seriously worry about cybersecurity-related liability from class action suits. Consider what happened to Anthem:

- In February 2015, Anthem announced that a cyberattack resulted in the theft from its databases of the personal information – e.g. names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses and employment information – of about 79 million people
- Plaintiff's lawyers filed a class action suit against Anthem, claiming it failed to adequately safeguard consumer's personal information.
- To settle the case, Anthem paid $115 million; and this payment does not stop injured consumers who opted-out from suing Anthem.

Plaintiffs' law firms are gearing up to bring class action suits against any large company that stores sensitive personal information – e.g. health insurers – and suffers a cyber attack. This is a real and growing threat for health insurers.

THE SOLUTION

Multidisciplinary enterprise risk management

You can't properly prepare for what you don't understand. And, it is unfair to expect your IT team – no matter how talented and diligent – to understand the complexity of quantifying your cyber risk and mitigating the risks via a tailored mix of cyber defenses, intelligent internalization of risk, and cost-effective insurance coverage. Instead, you'll need a multidisciplinary enterprise risk management program including extensive knowledge of your business operations, IT functions, IT security, privacy and cyber law, and insurance.

Not only will a multidisciplinary enterprise risk management program help protect your plan, it is regulatorily required:

- **HIPAA Security Rule:** Codified at 45 CFR Part 160 and Subparts A and C of Part 164, the Security rule requires health plans (as Covered Entities) to deploy a comprehensive cybersecurity program including "an accurate and thorough" cyber risk assessment.
- **Own Risk and Solvency Act (ORSA):** This NAIC model law has been adopted by 49 States. It requires some health plans to conduct at least annually a "confidential internal assessment . . . of [their] material and relevant risks . . . and sufficiency of capital resources to support those risks". Because cyber risks qualify as "material" for almost all health insurers, their annual ORSA report should address them, which at a minimum should involve conducting an accurate qualitative and quantitative cyber risk assessment, which the authors refer to as a Financial Harm Cyber Risk Assessment (see below for more detail).

- **Insurance Data Security Model Law:** In October 2017, the NAIC adopted its *Insurance Data Security Model Law* (#668). In Section 4, it mandates that insurers "develop, implement, and maintain" an "Information Security Program", which includes conducting a "Risk Assessment" to "identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction" of its "Non-public Information." Section 4 (C)(3) expressly mandates that insurers assess "the likelihood and potential damage" of cyber-attacks.

Plus, being fully aware that health plans' computing technologies are mission critical, many insurance regulators want to know how plans are mitigating their cyber risks; and they expect ORSA reports to address this topic.

Introduction to a cyber risk financial model

Often, the biggest stumbling blocks for health plans trying to improve their ability to prepare for cyber risks is that their current approach to enterprise risk management doesn't include a financial model that facilitates the proper assessment of cyber-attack risk; that creating one can be very difficult because of the complexity and significant uncertainties; and they don't know how to conduct a cyber risk assessment that identifies and QUANTIFIES their risks (known as a Financial Harm Cyber Risk Assessment). These stumbling blocks make it more challenging for health plans to:

- Adequately quantify cyber risks;
- Make good decisions about its cybersecurity defenses; and
- Properly decide which cyber risks to internalize and which to insure.

Our discussions with insurance executives and the NAIC revealed that health insurers are not consistently quantifying cyber risks as part of any risk assessment; sometimes not even attempting to do so. This is not surprising, because almost all cyber risk assessments done by third-parties focus almost exclusively on interference risks (i.e. technological, people, or process vulnerabilities that can "interfere" with your operations).

The good news is that cyber risk is quantifiable, and that many health plans already use indicators that can help them assess the financial impact of a cyber-attacks. Health plans have experience modeling what would happen if they lost membership, were unable to manage care (through prior authorization, referrals, or other processes that are technology dependent) or failed to meet contractual obligations. Additionally, health plans can leverage the publicly available information about the financial harm that companies in other industries suffered from cyber-attacks, including (among others) the Ponemon Institute Research Report "2018 Study on Global Megatrends in Cybersecurity;" the annual NetDiligence Cyber Claims Study; and the annual BakerHostler Data Security Incident Response Report.

The authors created a financial model that tested high, medium, and low impact scenarios for an illustrative health plan experiencing a cyber-attack that impacted systems for 10 day period. We grouped the financial harm from cyber-attacks into four categories (see diagram on page 1):

- **Increased claims** – from the inability to support utilization management;

- **Fines & penalties** – from failure to meet service level agreements and having to pay claims interest and breach penalties;
- **Lost revenue** – from membership decreases due to the inability to underwrite claims and reputational damage; and
- **Increased administrative costs** – from paying for a corrective action plan (e.g. cyber investigation, remediation, notification, and public relationships), litigation and regulatory fines, and credit monitoring.

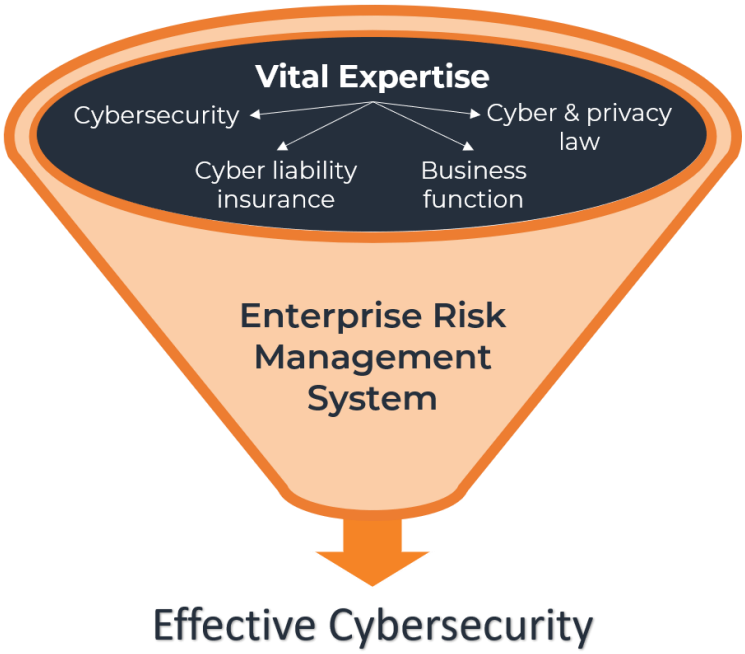
The low impact scenario assumed data were recoverable and were not obtained by the attacker, not all systems were down allowing for some utilization management efficiencies, and few performance guarantees driving financial penalties. In the high impact scenario significant costs were associated with per beneficiary penalties for a breach and lost membership due to the system unavailability during a peak enrollment period. We assumed a 2% margin on premium and 4% contribution to fixed expense (i.e., 8% administrative expense ratio driven by 50% variable and 50% fixed costs). The analysis highlighted the variability of drivers across plan and that many risks can be mitigated by planning. This is why financial risk assessment is such a vital part of a thorough ERM for health plans.

Introduction to a financial harm cyber risk assessment

Though it is not stated this way often enough, the goal of all cybersecurity is to prevent cyber-attacks from inflicting financial harm or otherwise impeding an organization's mission. While there's no one-size-fits-all approach to cybersecurity, almost every expert agrees that an effective strategy should include an assessment of an organization's current cyber risks. This is typically called a cyber risk assessment.

But, most cyber risk assessments focus predominantly (or exclusively) on Interference Risks – namely, the risks that cyber-attacks will "interfere" with the availability, confidentiality, or integrity of your information systems or electronic data. This type of assessment is important; and to be done correctly requires strong cybersecurity expertise. This type of assessment, however, divulges too little about your financial risks and how to properly mitigate them, leaving you uncertain about how to best allocate your limited resources to protect your business operations and mission from cyber-attack.

In contrast, Financial Harm Cyber Risk Assessments deploy (1) proven Enterprise Risk Management principles and (2) expertise in cybersecurity, privacy & cyber law, business function, and cyber liability insurance.



Financial Harm Cyber Risk Assessments are customized to your people, business operations, IT systems and insurance.

They start by listing the ways that cyber incidents can inflict financial harm on your unique business model, including probability and fiscal impact of different cyber incidents. They include an Interference Cyber Risk Assessment that assess the processes, policies, people, and technologies that comprise and protect your electronic information systems and electronic data – looking for vulnerabilities and improvements. They predict your potential out-of-pocket costs from cyber incidents by analyzing your insurance coverage. And, they suggest cybersecurity improvements and additional insurance coverage -- including quantifying the value and costs of making them – that can help you better mitigate your cyber risks.

The relationship between a financial harm cyber risk assessment and the Risk-Based Capital Formula

As detailed above, cyber-attack poses significant financial risks for health insurers. However, projecting and preparing for the financial harm from cyber risks is complicated by the limited historical patterns of cyber-attack, the lack of related financial harm data, and the fact that this limited information might not be predictive of future cyber attacks. Plus, health insurers also struggle to frame the impact of a cyber-attack on solvency because they rely heavily on the Risk-Based Capital Formula ("RBC Formula") to evaluate their risk capacity.

The RBC Formula is a method to measure the capital an insurer needs to support its overall unique business model including asset risk, underwriting risk, and other risk (including operational risk). According to the NAIC website, "RBC is intended to be a minimum regulatory capital standard and not necessarily the full amount of capital that an insurer would want to hold to meet its safety and competitive objectives." Insurers need to leverage additional methods and standards to evaluate capital

adequacy in light of strategic, environmental and other business impacts, which is exemplified by the limitations of RBC in evaluating cyber harm. Currently, the RBC Formula uses a catch-all charge of 3% to account for operational risk (which includes cyber risk among other business risks).

According to discussions with the NAIC representatives, separate or sub-charges for cyber risk may be incorporated into future adjustments to the RBC formula. These changes will require improvements to the way organizations quantify their cyber risks.

Therefore, the current RBC Formula, by itself, is insufficient to estimate the impact of a cyber-attack because it places a relatively low weight on operational risk. A financial harm cyber risk assessment addresses this gap. Insurers who have experience quantifying loss scenarios that have educated their risk management programs and been leveraged to stress test capital adequacy will be better prepared to meet the expectations of their boards and regulators in response to future changes to the RBC Formula.

Tips for creating the right financial model and conducting a financial harm cyber risk assessment

Tips for the assessment itself: A Financial Harm Cyber Risk Assessment should start by listing the ways that cyber incidents can inflict financial harm on your unique business model, including probability and dollar value of different harms. They include an Interference Risk Assessment, namely, assessing the processes, policies, people, and technologies that comprise and protect your information systems and electronic data – looking for vulnerabilities and improvements.

A Financial Harm Cyber Risk Assessment requires an inventory of contractual penalties and other applicable fines and adds costs associated with credit monitoring, reporting, and litigation. Review contractual penalties and potential interpretation carefully to evaluate the potential definition of a breach and whether fines are per episode or per beneficiary. The inventory is leveraged to build scenarios that will stress test the limits of the organization's cyber insurance policy (assuming they have coverage and its capital. Analysts should also consider reputational risk and potential loss of business due to a breach.

The final step is to stress these harms against the limits of your insurance policy and available capital. One approach to stressing capital is to deduct the losses from breach scenarios from surplus and comparing the result to your organization's authorized control level (ACL) to estimate RBC impact.

Tips for your internal team: Organizations should achieve broad, multidisciplinary staff participation in managing cyber risk. Leadership should understand their compliance program and how each function is impacted and there should be consensus on strategic investments. For example, the CFO will be aware of compliance efforts and will likely have been engaged in purchasing cyber insurance. However, in the case of a material breach, they may find themselves inadequately prepared to evaluate financial implications particularly if they do not know of penalties built into contracts or the corporate position on ransom payments. Hence, legal counsel is often needed to assess contractual penalties; and, if they have privacy and cyber law expertise, they'll often be the best suited to project costs related to investigation

and legal and regulatory liability. Moreover, health plans will benefit from the involvement of someone expert with their cyber liability insurance (or overall insurance coverage if there's no cyber policy).

Find a good partner: When it comes to Financial Harm Cyber Risk Assessments, it is important that health insurers not rely solely on their own analytical inputs. Instead, they should engage an outside expert. Unfortunately, few cybersecurity vendors (1) understand how health plans operate and (2) possess the rare mix of ERM, legal, cybersecurity, and insurance expertise to help health insurers thoroughly assess their financial risks from cyber-attack. The solution is to make sure that whoever is conducting your cyber risk assessment understands your business model, has the requisite expertise, and delivers a written assessment integrating Interference Risks and Financial Harm Risks. Health plans will be able to use this type of assessment when completing ORSA Reports, interacting with insurance regulators, and (if ever called upon) to prove they complied with HIPAA, the NAIC's new *Insurance Data Security Model Law*, and other privacy laws (e.g. the GDPR and New York's Department of Financial Services Cybersecurity Requirements).

Contact Practical Cyber:

Elliot Turrini – Elliot.Turrini@PracticalCyber.com – (201) 572 4957