Fred C. Church, LLC. and BeyondTrust Cyber Insurance Webinar – March 23, 2022

Live Audience Q&A

Question: What do you do with the questions in the surveys that are not applicable to your infrastructure?

    Chris: Most security questionnaires have a N/A option, but you must provide feedback as a requirement as to why you marked it N/A.

    Tom: We encourage our clients to complete an addendum document (a simple word document) along with the application where they can clarify their answer to any question that does not perfectly relate to their industry, network infrastructure, or other circumstance.

Question: Are you seeing that the cost of ransomware is exceeding the total value of insurance availability? That is, if my company has $5M in insurance, but typical ransomware is more akin to $10M. How should companies factor in the actual risk vs. the coverage?

    Tom: While there have been ransoms that make the news that get up into multiple millions, most demands settle for something in the $100,000 - $300,000 range. This is very dependent on the size of your organization so it’s hard to pin down an exact answer to this. But, one thing we do know is that these threat actors are sophisticated and their number one goal is getting paid – so, they’re incentive to request a ransom that they think the organization can pay. Understanding what your probably maximum loss is given your IT infrastructure – particularly your backups, will help determine what limit you can buy to transfer the risk of the financial impact of a loss that you cannot mitigate through your own backups procedures.

Question: Speaking of ransomware, do you recommend paying the ransom?

    Chris: Paying Ransomware is the last thing anyone wants to do, but in order to avoid paying the ransom, there needs to be some key elements in place to mitigate having to pay such as a full Disaster Recovery and Business Continuity plan. If you don’t have valid backups, if you don’t have a plan in the event something like this occurs, and you haven’t testing it to make sure it works or validated it, companies are left with no choice but to pay it. Larger companies typically have very mature security and IT Infrastructure programs in place that in most cases will address this, but it’s impossible to think about every single thing, because if they did, they wouldn’t be in the position. This is why we put so much emphasis on security.
Question: If you're an MSP, do they take into account if your clients are on 2FA?

Tom: This is a good question that I do not have particular insight into, but generally speaking carriers like to see MFA wherever and whenever possible – a zero trust environment is the best environment.

Question: Obviously, we can't rely on insurance to mitigate the risks of cyberattack, especially ransomware. What are your recommendations for companies to prepare and defend themselves from such attacks. (I know that's broad - but what do you recommend as an overarching security strategy.)

Chris: Great Question – In most cases companies will follow a framework for this security program, some follow NIST, some follow CIS Controls, some MITRE, and these are just a few. All of them have slightly different ways at approaching security but at the core they all do the same, which is prepare a company's security program to protect them against bad actors. This is where I would start, look at the various frameworks, depending on your industry, and then build your security program around it.

Tom: Following best practices for implementing security controls, creating and testing an incident response plan, and maintaining a comprehensive employee security awareness program are great steps to mitigate your risk.

Question: Slide 10's title is "targeted attacks" but are these attacks attempted, or attacks that succeeded?

Chris: Great Question – Coveware provided the statistics, I don’t want to misspeak on their behalf.

Question: Does BeyondTrust handle multi-tenant configurations? Can an MSP host the services on their Cloud.

Chris: We are currently single-tenant cloud configuration, but we do have options in the marketplace for you to host in your own private. Our roadmap will have something in the future for multi-tenant, but with anything else, multi-tenant has its own set of risk factors especially when it comes to Privileged data. Most security questionnaires specifically ask about single tenant and data privacy. So while I understand the multi-tenant use case, it does have its own downfalls.

Question: Thoughts on MFA for internal users. We use it for our Administrators and for VPN connections. But is MFA necessary for general users that are in the office.

Chris: I highly encourage companies to enable MFA wherever possible. I know we always think of administrators as the ones with privileges, but when we consider the basic user, their account, and everything their account has access to, technically that account has privileges to. You need to review an average user, what a typical account has access to – HR System, Intranet, Company Apps, maybe something that doesn’t require an Admin login, but is still considered a privileged account because of what they access. In the event that ID was compromised, what does that account truly have access to and how
much damage could that do within the company if it was in the wrong hands, otherwise, why would everyone be worried about locking their computer when they left, if that account doesn't have access to anything, why lock the computer for security purposes?

**Question:** are there cyber insurance companies that are better than others? ie: we have cyber insurance from the same company we have general liability...when we have a breach is our insurance provider knowledgeable enough to help us in the best way possible?

**Tom:** Not all carriers are created equal. This is where a good insurance agent comes in to play. Many carriers have a cyber insurance offering, but not all truly specialize in it. Some key things that you can look at on your policy to see if you have good coverage are:

- Full limits for Ransomware/Cyber Extortion with no coinsurance.
- Full limits for Business Interruption
- At least $1M for Dependent Business Interruption

**Question:** When you say that providers want MFA, are they looking for it for cloud (i.e. MSO365), or also for internal network A/D login credentials?

**Chris:** I would say they are looking for any type of login to datasets whether it be local, in the cloud, applications, etc... be configured with MFA authentication.

**Tom:** Yes, the carriers are primarily concerned with MFA for email, remote network access, and privileged/admin access. But, MFA for cloud access where possible is important as well.

**Question:** What are the top 10 reports that your insurance may ask you for so you can do your due diligence ahead of time?

**Tom:** Get a ransomware supplemental application early. Consult any 'no' answers with you internal and external IT teams and review with you business leaders to see if these things can be implemented.

**Question:** What are the Top 10 things companies can do to help reduce cyber insurance premium?

**Chris:** Unfortunately, there is no secret recipe for cyber insurance, there are far too many factors that go into it... The most tangible item available right now is the Ransomware Supplemental Addendum/Application. From my perspective, I don't want to speak for Tom, but cyber insurance is looking for positive responses in all 9 categories to even be considered for coverage. Without a positive response/answer to what "YOU" as company are doing, there is far too much risk for a broker to insure. So the first thing I would ask your organization to do, is to respond to the RSA, and then possibly even use the benchmark Tom provided and see where you are.
To: Chris, agreed on all points. I'll add that while it’s unlikely that your insurance premiums will go down year over year (at least for the time being), you can best manage how much they go up by presenting the best possible cyber risk profile to the marketplace. A ransomware supplemental application showing key controls are in place is big factor in this: MFA (for email, remote network access, and privileged/admin access), Backups (that are encrypted and kept offline or in the cloud), EDR, Employee Awareness Training, and a Cyber Incident Response Plan (that has been tested). These 5 key controls are a great start.

Going beyond those baseline controls, the best pricing will go to companies that have a 24/7 security operations center (whether in-house or third party), have total control over their privileged and service accounts, can show a proper patching cadence, and have no exposure to open ports – most carriers do some kind of external vulnerability scan that detect these things. A good score helps push you into that best pricing category.

**Question: Do insurers actually offer lower premiums if an infosec program is determined to be "excellent," or is the premium amount relatively static, and it's only a matter of whether a company is able to obtain insurance or not obtain it?**

Tom: Companies with the best cyber risk profiles will get the lowest available premiums. There is no direct relationship between controls and premiums savings like a safe driver credit on auto insurance or a sprinklered building credit on property insurance. But, if your agent is marketing your coverage to multiple carriers (which would be a good thing to do after investing in your network security infrastructure), then that can pay off in terms of you getting the best premium available in the marketplace.

---

**Meet the Presenters**

**Tom O’Neill, Management Liability Coverage Specialist, Fred C. Church**

Tom O’Neill joined Fred C. Church in 2019 as the coverage specialist for Cyber, Management Liability, and Professional Liability coverage lines. In coordination with the commercial insurance client executives, he regularly consults with clients about their risk management strategies and cybersecurity mitigation efforts.

**Christopher Hills, Chief Security Strategist, BeyondTrust**

Christopher L. Hills has more than 15 years’ experience as a Senior Security and Architecture Engineer operating in highly sensitive environments. Chris is a military veteran of the United States Navy and started with BeyondTrust after his most recent role leading a Privileged Access Management (PAM) team as a Technical Director within a Fortune 500 organization. In his current position, he has responsibilities as a Senior Solutions Architect consulting on PAM implementations and reports to the Office of the CTO as Chief Security Strategist for the Americas. In his free time, Chris enjoys spending time with his family on the water with their 32-foot speedboat in the summer and taking to the sand dunes and off-roading in the winter.