WEBINAR Q&A SUMMARY

Cybersecurity for your Business: Where to Begin

QUESTION

- If you are hypothetically the victim of a ransomware attack, do you pay?
- And if you can justify the cost of paying, does this validate the criminal's model and expose everyone to further risk?
- Can the data you recover be considered safe?

ANSWER

1. One should never be put in a position to be required to pay. But it requires that you're prepared. Preferred approach is never to engage or pay, but that is changing.
2. If you do pay, then ethics comes into play. If we do start paying to recover from ransomware, then criminals get payouts and incentives. Therefore, there is negative feedback at play (positive for the criminals). Boils down to this: Be prepared. If my protection mechanisms are in place, then I should be able to quickly recover without having to pay.
3. Get yourself in a position to never have to worry about this.

QUESTION

- What is the greater risk, physical security or Cyber security, and how much should I spend on each?

ANSWER

- Physical security is intuitive. But paying for cyber security is not as intuitive. There should be an upfront investment at the get-go.
- How much to spend on each? Depends. Ultimately, both need to be considered. Cyber security should be an intuitive response. We need to change the language.

QUESTION

- Does WBM have a security incident response process to share as an example?

ANSWER

- We do have these, and would be happy to share. Sharing helps everyone. Please contact your WBM Account Manager for more details.

QUESTION

- Can you share your thoughts on the idea that small/medium businesses may think that they aren't targets for cyber attacks?

ANSWER

- Size of business as variable is irrelevant. This is a financial investment from the criminal's perspective. So everyone is a target, so long as you have valuable information.

QUESTION

- Where should an organization go to learn more about the Cybersecurity Insurance offerings?

ANSWER

- Go to your own insurance company. They should have these already

QUESTION

- One the key elements of protecting your business is under People, end user awareness, in your experience what is the most productive method?

ANSWER

- People Controls was the first recommendation we shared. Most productive is having professionals talking to people. But it's impractical to scale. Town halls are great.
- Use online awareness training programs, this will expose the weak spots. Then you can target online training courses.   Awareness is key.

QUESTION

- You identified Government as a common threat... Can you please give an example of how government can be a cyber threat?

ANSWER

- Governments are using cyber warfare on a global geo-political scale.   These are about gaining competitive advantages or social disruption.
- Governments are scary because they have the luxury of time.   But plenty is also being spent on defense. You can find plenty online on this topic.

QUESTION

- Would you be able to provide some suggestions of reputable online end user training that could be used not only in orientation by regular staff training?

ANSWER

- We can definitely share this information. Contact your Account Manager for more details.

QUESTION

- WBM is our company's IT provider. Does WBM have posters, articles, etc. that we can share with the end-users in our company to raise awareness on what they can do to avoid cybersecurity attacks?

ANSWER

- The use of printed versus online material depends on the physical restrictions of the business. If all end users are in central locations, the traditional printed collateral is effective.
- However, if the workforce is distributed, do online live training. Use a combination of resources.
- Have someone responsible within the organization to drive this and work a multi-dimensional approach that is specific to your own organization.

QUESTION

- This all sounds EXPENSIVE! What would you say would be the cost-effective way to begin our CyberSecurity enablement road ahead for those that have not had a strong practice?

ANSWER

- It sounds expensive, but it does beg the question of “what does it cost to not do anything”.
- Being cost effective - you can staff internally and have an individual driving the strategy.
- Or look at Managed Services providers. Look at doing it "as a service". A good MSP will grow with you "as a service". And this is a good way to get started down the path of Hybrid IT / Cloud integration.

QUESTION

- As our IT service provider, how is WBM protecting their clients in the event WBM suffers a cyber attack?

ANSWER

- We are a target like anyone else. We apply the principles that we talked about today.
- We have multi-level protections exactly as we discussed today. People, Technology, and Process controls. Risk, controls, standards…

QUESTION

- What is the best way in your opinion to get C Level support to expand a cybersecurity program with the increased activities from the dark side.

ANSWER

- A fairly effective way to get C level support is to use the results of a security assessment that includes penetration testing. When C level executives are presented with a comprehensive list of recommendations based on real life testing, it is difficult to ignore the real and present risk.
- One caveat here is that the security assessment has to produce convincing material backed up with penetration testing results.
- Finally, look for assessment reports that provide financial projections on the cost associated with implementing recommendations. It is more effective to state "WE need to do X, and it is going to cost us Y. And we don't do X, we are faced with risk Z.

QUESTION

- I hear a lot about "it's not if but when" but I'm starting to hear a new one which is "you're already compromised, you just don't know it". What are your thoughts on that?

ANSWER

- That is a very real concern. It is expected that there is small chance that defensive measures will fail. If that happens, there needs to be different mechanisms to detect breaches.
- In the Cybersecurity industry, we call this Breach Detection. As an industry segment it has some long- standing vendors and also some new and innovative vendors that provide interesting approaches by using AI and machine learning techniques to detect anomalies (or deviations from normal) within your infrastructure. Once detected, Breach Detection systems can isolate components from the network or simply alert for follow up (protection versus detection).