Cybersecurity: The Way Forward

This handout is designed to complement the cyber security presentation by Vince Crisler, Dark Cubed's CEO and Founder. If you would like a copy of the slides for the accompanying presentation, please e-mail info@darkcubed.com.

#1. Two factor is not optional

A simple username and password no longer provides enough security. If you are protecting your sensitive systems (e.g. customer data, e-mail, patient data, payments and banking, social media etc.) with only a username and password, then you are going to face a breach.

- ❑ Implement two factor authentication on e-mail.
- ❑ Identify corporate systems that store and process sensitive data (medical records, customers records) and implement two factor authentication on them.
- ❑ Implement two factor on banking and payment systems.

#2. The basics matter

Just like we recommend key activities for our patients hygiene, we need to do the basics to protect the security of our systems. There are simple things that can help make a cyber attack less likely. In fact, some of the most technically simple solutions can have the greatest impact in reducing your organizational risk and minimizing the damage if an incident does occur.

- ❑ Use antivirus/antimalware on all systems and require that they update automatically.
- ❑ Make sure all desktops and laptops are the current version of the operating system and require that they auto-update as patches are available.
- ❑ Deploy a firewall and make sure someone qualified to configure it checks on it quarterly.
- ❑ Require computers to lock after 15 minutes of inactivity at a minimum.
- ❑ Run simulated phishing exercises to teach your employees how easy it is to accidentally fall prey to a targeted phishing email.

#3 Pay attention to what is coming in and out of your network

Many breaches could be detected faster if companies collected data on what is coming in and out of their network and looked for anomalies in that traffic. Such data can be produced by your firewall.

- ❑ Make sure you are storing at least 30 days of logs in some format (ask your IT team about a syslog server).
- ❑ Have someone review this data at least monthly for foreign or suspicious traffic. This can be accomplished at a basic level for a low cost.

#4 Know your data and secure It

Often data breaches involve data that companies just simply do not use anymore. It is important to know where sensitive data (PII, HIPAA, PCI) is being stored on your network and to routinely delete old, unused data.

- ❑ Run a data "census" to search for locations where sensitive data might be stored; this is a good job for summer interns!
- ❑ Advise all employees and staff to only store data in approved locations, hold them accountable.
- ❑ Encrypt sensitive data using strong passwords; there are many low cost ways to accomplish this important security measure.
- ❑ Delete data that no longer has business value in accordance with any applicable regulations which your business operates under.

#5 Segment to save it

The most exciting thing for an attacker to find is a wide-open network where user machines are on the same network as servers or other sensitive systems. Your IT provider should know how to separate these systems on distinct networks to slow down the attacker.

- ❑ Do not allow personal machines or mobile devices to connect to the company network.
- ❑ Ask your IT provider if your servers are on a separate network from your desktop computers.
- ❑ If you have a data center, you should have a firewall protecting the data center from the rest of the network.

dark3

#6 Have a plan and test it

While cyber security may feel overwhelming, pulling your leadership team together for a couple hours of discussion can go a long way. Search for headlines on cyber attacks in your industry and ask yourselves what you would do if that happened to you.

- ❑ Just thinking about how you would respond can save your team major headaches when a cyber incident does occur.
- ❑ Figure out who would take the lead, who would be in the room for the discussions, and who would make the final decision.
- ❑ Partner with your IT team to get their inputs and ideas.

#7 Know who you are going to call

Having your cyber security vendors identified ahead of time will save you valuable time and energy. Do a little research on the vendors other companies like yours are using and introduce yourself to those vendors. Building the relationship before an incident is a critical factor to success.

- ❑ Identify the cyber security company that will do forensics and incident response when you need help.
- ❑ Consider who will provide legal support and public affairs support and make sure they are prepared.
- ❑ Consider getting cyber insurance to help cover losses and damages, but also to get access to a team of companies that can help you respond.

#8 Recognize the overlap of digital and physical security

Do you keep your sensitive IT assets physically protected? Sometimes an unlocked door or a stolen device can have more impact than a digital attack. Make sure you are thinking about how devices could be stolen or unauthorized access could be gained due to weak security.

- ❑ Make sure all of your laptops and mobile devices are encrypted; this should be an easy, low cost measure to implement.
- ❑ Lock IT rooms and consider using motions sensors or cameras to manage unauthorized access.
- ❑ Either deactivate unused network ports of place plastic locks in them to prevent unauthorized network access.

#9 Train your employees

One employee making a good choice can be the difference between a thwarted attack and a data breach. Equip your employees with information on which attacks are likely and who should receive reports of suspicious activity. There is extensive amounts of free information available on cyber security training if you look for it.

- ❑ Make sure employs know who should receive reports of suspicious activity.
- ❑ Train employees how to avoid phishing attacks and to avoid downloading potentially malicious files.
- ❑ Encourage employees to teach their kids/parents. Sometimes we learn best by teaching others.

#10 Don't be embarrassed!

At some point even the most secure companies suffer an incident. Talk with other companies and your peers and learn about their experiences with cybersecurity. We are stronger together, and only by working together can we be prepared.

"Success is going failure to failure without a loss of enthusiasm" – Winston Churchill

This document was prepared to accompany a presentation by Vince Crisler, CEO and Founder of Dark Cubed. These ten items represent key areas of focus for any small or midsized organization to get started on improving security and is not intended to represent a complete security program. Dark Cubed makes no representations or warranties as to the accuracy of this information and assumes no liability.

Contact Us!

info@darkcubed.com
@darkcybedcyber