Cybercrime Survival Guide — A 3-Step Process

by **Reg Harnish**, CEO, GreyCastle Security

Cybercrime has reached epidemic proportions. Hospitals, colleges, banks, retailers and all other types of businesses have found themselves under continuous attack by threats whose motivations are high and capabilities are even higher. These victimized organizations often experience business interruptions, lost productivity and massive expenses as a result of cybercrime.

The reputational damage can be far worse.

The erosion of brand trust resulting from cybercrime is not well understood. Public and crisis communications teams are faced with explaining a complex issue to audiences that know little about the subject matter, and honestly don't care. These same audiences are being inundated with breach notifications from the credit unions, grocery stores and restaurants they use. The problem seems unsolvable.

Despite all of this, there are several important things that any business can — and should — do to help prevent cybercrime and minimize the damage from security breaches and incidents.

The first is understanding your business' cyber risks. This is a simple process called a Risk Assessment, which identifies organizational weaknesses and the threats that may exploit them. It then applies simple math to these discoveries, including the likelihood of exploitation and the impact on the business if that exploitation occurs. The result is a short, highly prioritized list of cybersecurity efforts that the business should focus on.

The second is near and dear to communications professionals — change your employees' behaviors. Employees, and people in general, are the single greatest problem in cybersecurity today. From careless downloads to accidental sharing of classified information to clicking malicious links in emails — people are a major challenge for cybersecurity professionals all over the world.

Addressing people risk requires an effective, continuous, engaging and practical cybersecurity awareness program. The program should measurably change employee behaviors through education, training and testing of cyber skills.

The last, and perhaps most important, is building a response capability. Due to the asymmetric nature of cyberwarfare, it is not possible to prevent all attacks. This is true for the same reason that sporting events don't end in 0–0 ties — offense is easier than defense. Businesses must figure out how to increase their resilience to cyberattacks in an environment where they truly cannot protect all of the things that they would like to.

The cybercrime industry is massive and growing quickly, and things will not get better before they get worse. Organizations should develop and test an Incident Response Plan (IRP) that helps formalize the activities that are performed following a breach or incident. Responders should be trained and tested on a regular basis. This is perhaps the single most important investment any business can make today.

Every day we are besieged with headline after headline detailing how another university, hospital or retailer was breached. The very nature of cybercrime makes it difficult to predict where the next attack will come and what it will look like. One thing we can count on, however, is that IT WILL HAPPEN.

If we expect our businesses to survive cybercrime, we must all become part of the solution.

GreyCastle Security is a cybersecurity consulting firm focused on risk management, awareness and operational security. The company was established to counter rapidly evolving cybersecurity threats and manage risks in people, processes and technology. GreyCastle Security is comprised exclusively of highly certified professionals with prior security experience in health care, education, retail and gaming. Team members represent former CISOs, ISOs, security specialists and operators.

For more information about GreyCastle and its service, visit their website at www.greycastlesecurity.com/ or contact a associate at the firm at sales@greycastlesecurity.com, or call (518) 274-7233.