Burrus Research®

Beating Cybercrime Before It Happens To You

To understand why cybercrime is rapidly growing, as well as the seriousness and impact it can have, we need to compare it with the more traditional and visible aspects of street crime. If we were to break it down into the business language that we all understand, what is the ROI of crime both online and offline?

Robbing a physical bank does offer potential rewards to criminals, but at a very high level of risk including getting shot. There will most likely be witnesses and CCTV footage that will increase your chances of getting arrested or jailed. There are usually helpers who can also be caught or killed including a get-a-way car driver and people who will give you cash in unmarked bills for whatever you have taken; you get the idea, the list often goes on.

Online crime on the other hand is a different story offering much lower risk and much greater reward. For example, cybercrimes are not usually detected right away, sometimes taking weeks or months to discover. There is a lack of eyes observing the act, and because it is often carried out from another country, it is notoriously difficult to track and locate online criminals.

Legal systems throughout the world differ significantly, and even if online criminals are caught, the likelihood of being able to extradite them is not as easy as authorities would like. When looking at crime through business eyes, it's easy to see why online criminal activity is the fastest growing crime in America.

Technology has famously disrupted industries across the globe, but the criminal underworld is not an area that immediately springs to mind. Crime figures released by law enforcement agencies will often reveal a significant drop in traditional crime but seldom include victims of online crime. The crime rate in England and Wales soared when they made the brave decision to include cybercrime for the first time.

The increase of high profile data breaches has recently put cyber security on the map. Rather than waiting to be the next victim, companies need to go beyond reacting and responding to attacks, and consider using new tools to predict and prevent the crime, including behaviour analytics. In addition, real-time analytics and deep learning algorithms can learn from every cybercrime ever committed to detect and ultimately prevent new variants attacking a company network.

The rise of Cognitive Computing from tech leaders such as IBM Watson alongside advances towards quantum computing will usher in a new age of collaboration. Security as a service (SECaaS) will encourage working together rather than alone. Company to company and organization to organization, there is a realization that learning together is better than learning by ourselves.

If every attack experienced was fed into one central repository so that every conceivable pattern of attack was analysed and learned from, it would be a significant step forward for the good guys.

Traditionally people do not change their lifestyle habits until the doctor tells them they are obese and need to take action. Equally, many seldom invest in home security until they have been burgled. These are textbook examples of a reactionary mindset and something we need to change sooner rather than later.

We need to snap out of the out of sight, out of mind mentality and understand that it would be much easier to be anticipatory and pre-solve predictable problems. For example, there has not been a high profile mobile cybercrime yet. It is relatively easy to predict that there will be a major mobile hack or cybercrime in the very near future. Do we wait until it happens before reacting or prepare for it right now?

Our primary computer has evolved from a desktop PC to a laptop and now to a mobile smartphone or tablet. For this reason alone, we know for certain that this will be where many future attacks will occur. This is a wake-up call to become anticipatory by adopting a predict and prevent strategy to prepare now before it happens.

The golden rule to remember is that if it can be done, it will be done, so why let it happen to you? Would you rather your company be caught in the headlines reacting to an attack that is featured on every news channel in the world? Or would you sooner be the organization that walks away with its reputation still intact?

Educating employees, as well as investigating new options such as Cognitive Computing and deep learning algorithms, as well as behavioural analytics that can shut down threats within a few milliseconds, are just a few of the small steps you could be taking today. The only question that remains is, why aren't you acting on this now?

Cybercrime has a much higher ROI for criminals than physical crime, and that means it is evolving alongside our digital lifestyle, and the technology we take for granted could easily be used against us. It's time for you to take a closer look at what you are doing now to prevent a future problem. Will you be anticipatory or reactionary? The choice is yours.

About the Author:

DANIEL BURRUS is considered one of the world's leading technology forecasters and innovation experts, and is the founder and CEO of Burrus Research, a research and consulting firm that monitors global advancements in technology driven trends to help clients understand how technological, social and business forces are converging to create enormous untapped opportunities. He is the author of six books including The New York Times best seller Flash Foresight. This article is reprinted with permission. Reproduction without permission is strictly prohibited. For reprint permission, contact Burrus Research, Inc. at office@burrus.com.

INOVA BUSINESS SCHOOL

INOVA CONSULTING