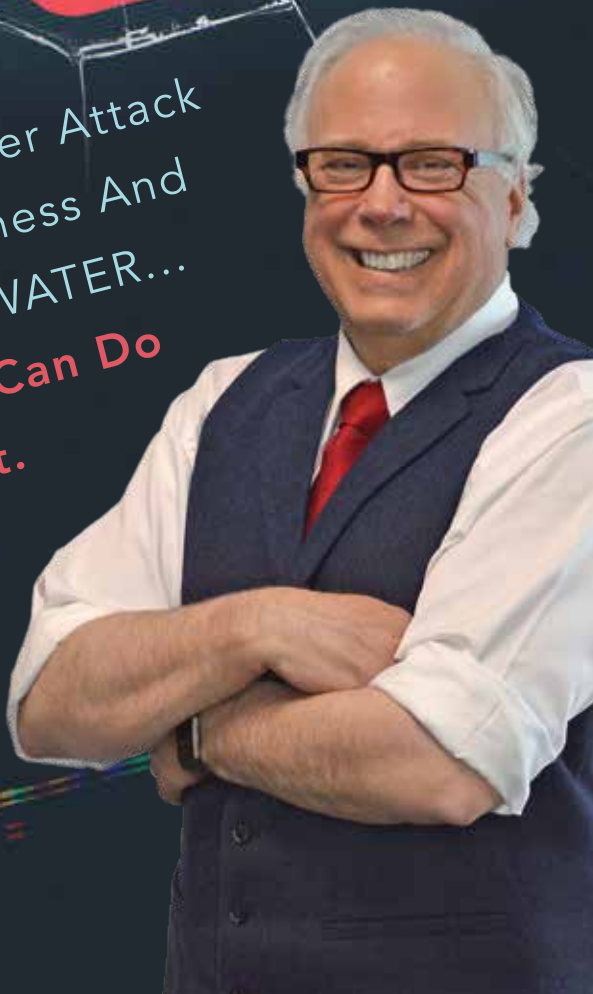
ON THIN ICE

How Just ONE Cyber Attack Can Put Your Business And Finances UNDERWATER...

And What YOU Can Do NOW To Stop It.



Tony Olson

History Of Cybersecurity

A SPECIAL EXCERPT FROM THE
AMAZON.COM BOOK

CHAPTER 1

HISTORY OF CYBERSECURITY

BY TONY OLSON

Over the history of mankind, whenever something new has been developed for good, there have been people that have twisted that new functionality and redeployed it for evil.

Computers have not been immune to this twisting of good for evil intention. In fact, by their very design, they serve as the perfect vehicle to distribute evil-concocted payloads. Today, computer devices have been universally deployed. Some estimate that there are 24 billion compute devices in the world today. These devices are all connected on a worldwide scale. This tremendous and ever-expanding computing and communication power, has turned out to make the perfect tool to enable, amplify, and spread anyone's evil intentions rapidly and globally.

In the short history of computers, the number, cost, and scope of cybercrimes committed have taken off like a rocket. And these evil efforts continue to escalate exponentially. Over the last forty years, we have already gone through what I categorize as the 4-movements of cyberdisruption:

1) **Cyber Curiosity**
2) **Cyber Criminality (Theft)**
3) **Cyber Espionage, Terrorism & Warfare**
4) **Cyber Organized & Commercialized Crime**

CYBER CURIOSITY

The initial opportunity for someone to disrupt other people's lives using a remote computer came about when the first computer network link was established on October 29th, 1969. The network was called the ARPANET, and it was funded by the United States Department of Defense. Even though this early computer network was on a closed-circuit system consisting of three computers that were being used only by scientists, it still served as the earliest laboratory project for cybersecurity.

During an ARPANET research project in 1971, Bob Thomas conceived of the possibility of a computer program moving across the network from one computer to another. This idea had great practical potential, for example, deploying useful programs remotely across the network to numerous systems. He created a small program to test his idea. His test program made that journey, and as it traveled, it left proof that it had been there, by printing a message on the local TENEX terminals. The printout said, "I'M THE CREEPER: CATCH ME IF YOU CAN." This program, now referred to simply as "The Creeper," was the first computer virus.

Another computer scientist, Ray Tomlinson, saw the Creeper program in action. He further advanced the idea by making the Creeper self-replicating. With this extension, he created the first computer worm. Then, Tomlinson wrote another program that was designed to chase the Creeper around the ARPANET and delete it, wherever it found it. He called this program the Reaper. It was the first antivirus program.

These three basic programs were created by two curious scientists with good intentions. They were simply working to advance the state of the art of network capability and communication. Even with humble beginnings, these three programs still today, serve as the model for most antivirus software.

That model, at its core, consists of four parts:

- First, identify a new threat.
- Second, write an antidote program to find it.
- Third, root it out and eliminate it.

- Fourth and finally, blacklist it so others will benefit from the knowledge gained by the operation.

While this method is effective, and it has worked well for many years, there is an inherent flaw in this model. That is, in this method of malware combat, the software must wait to develop an antidote until after a new threat has emerged. In other words, there cannot be a cure until after the disease has struck and is understood. Therefore, this method guarantees that some computers will always be infected by new forms of malware before it can be stopped.

One other fact of history that must be noted here is that the same Ray Tomlinson that created the Reaper program also conceived the idea of communicating from one person on one host computer, across the ARPANET to another person on a different host computer. This idea was the invention of email. Tomlinson had to design a new format for addressing the emails. He created the idea of using the format user@ host – a setup that is still in use today.

Why did I mention the invention of email at the close of this Cyber Curiosity segment? Because it is another perfect example of a development with good intentions being twisted for evil purposes. The invention of email was for good. It has gone on to positively impact the way the entire world communicates. Yet, at the same time, it has been twisted to serve an evil purpose. It has turned out to serve as a perfect vehicle for the delivery of malware payloads to the masses around the world.

Get the book to learn more about cybersecurity, its impact on businesses, and how to protect business assets.

Is Your Business Treading on Thin Ice?

It's not fair! You work so hard to grow your business, and all it takes is ONE cyber-attack from a hacker and your life (and business) is turned upside-down. In this important book written for today's business owner and CEO, you'll **learn the most effective cyber security solutions** to erect a steel wall around your business assets. You will learn:

- Why it's no longer a matter of IF small businesses JUST LIKE YOURS will suffer a cyber-attack, it's a matter of WHEN
- NINE critical steps you must take now to protect yourself from a data breach that could cost you MASSIVE money, time and quite possibly YOUR BUSINESS
- How to PREVENT today's fastest growing and most feared cyber-attack — RANSOMWARE — so you aren't blackmailed for TENS of THOUSANDS of dollars
- How to ensure YOUR OWN EMPLOYEES don't accidentally (or purposely) invite cybercriminals onto your network
- How to protect your IDENTITY from being stolen, how to keep your data safe in THE CLOUD, and so much more!

For more resources to protect your business from cybercrime, visit:

www.d2worldwide.com/information-technology