Interview:
"The real and growing threat of cyber crime to corporations"
CNBC Cambridge Cyber Summit

Stuart Madnick

Working Paper CISL# 2016-17

September 2016
The cyber threat is real.

If you have control of valuable assets, including trillions of dollars of transactions, as The Society for Worldwide Interbank Financial Telecommunications (SWIFT) does, your company will be attacked. It's a matter of when, not if, it will happen. That means you need to develop a sophisticated and multi-faceted approach to cyber-security.

Only a few years ago, corporate cyber-security might have been limited to installing the latest software patch—an activity on a par with, say, facilities management.

However, given the increasing number and magnitude of cyber-crimes, as well as new types of threats, cyber-security now requires a coordinated effort between companies, government agencies and advanced academics with cutting edge insights into the future of technology. In a networked world, no one can afford to go it alone.

"It is up to senior business leaders to take the lead in protecting their organizations."

-Stuart Madnick, Director, MIT’s Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

Register for the Cambridge Cyber Summit
While there still may be lone-wolf high school students hacking into systems in their spare time, most of the current serious attacks are initiated through use of an elaborate cyber-crime ecosystem. There, techies create cyber weapons that cybercriminals can buy on the "dark web"—often for remarkably low costs. Recently it has been reported that cyber weapons developed by the NSA were stolen and are up for sale.

Cybercrime poses a real and persistent threat to business, government and financial institutions. The February 2016 theft of $81 million dollars from the Bank of Bangladesh's holdings at the New York Federal Reserve via the SWIFT network serves as an important reminder of how effective and damaging these attacks can be. The thieves used the bank's own computers to make what appeared to be legitimate transfers of millions of dollars.

Attacks such as these are increasingly multi-pronged and require extensive knowledge of the organizations and systems being attacked.

For example: After the malware attack on the Bangladesh Central Bank sent the fund requests, it deleted the database record of the transfers, took steps to prevent confirmation messages from revealing the theft, and even altered the reports that were sent to the printer. Similar elaborate schemes were used in the December 2015 attack on Ukraine's power grid.

Although all the details of the Bangladesh event are not known, we do know that 50-80 percent of all cyber-attacks are aided or abetted by insiders, most commonly by an email message that asks a relevant party to click a link or open an attachment.

It is highly likely that almost everyone has received one of these Phishing attempts. Some are the fairly obvious: "I am a Nigerian Prince with millions to give you." These have a 1-2 percent success rate. Meanwhile, the more subtle "you have exceeded your email quota and you need to take this action to continue getting email"—can have a 10 percent success rate.

But, the real challenge is Spear Phishing, where success rates can exceed 70 percent. These are carefully crafted messages that appear to be coming from trusted individuals, such as a known executive in your company, and make use of detailed knowledge about you and your job.

Sophisticated threats and attacks such as these require a multi-pronged response. And while each organization will fashion its own customized response, we believe the all companies, institutions and government agencies should think holistically e2e, end-to-end.

It is up to senior business leaders to take the lead in protecting their organizations; and in the dark and complex world of cybercrime that can only be accomplished by working together with government, industry, and academia.