GlobalResearch
Center for Research on Globalization

The New Number One Problem for Mankind: Cyberwarfare and Human Error

By True Publica
Global Research, January 23, 2018
TruePublica 22 January 2018

Region: Europe, USA
Theme: Intelligence

Last May, Warren Buffett announced that cyber attacks are a bigger threat to humanity than nuclear weapons.

"I'm very pessimistic on weapons of mass destruction generally although I don't think that nuclear probably is quite as likely as either primarily biological and maybe cyber," Buffett said during Berkshire Hathaway's annual shareholders' meeting.

Interestingly, Buffett has put his money where his mouth is. In 2015, Berkshire made a bet that could profit from increased cyber breaches. Berkshire Hathaway Specialty Insurance launched two insurance policies that cover cyber liability and the costs incurred to respond to a data breach or threat.

Similarly, AIG launched a product earlier this year that covers expenses arising from online bullying and extortion, according to Fortune.

The writing is very clearly on the wall. In 2016, 6.4 billion connected things were in use worldwide in 2016, up 30 percent from 2015, and will massively increase to 20.8 billion by 2020. What follows next is a logical response to that explosive growth.

In 2015 cybercrime cost an estimated $24 million. In 2016 it rose tenfold to $209 million, in 2017 it rose twenty five fold to $5 billion and by 2019 most expert estimates put the cost of cybercrime exploding at a staggering four hundred times to $2 trillion dollars.

For perspective, the top five oil and gas companies in the world collectively have revenues of half that number. Similarly, so is 2017's record breaking global car sales revenue of the top five manufacturers. Global defence spending combined is three quarters of that number. That number – $2 trillion – is truly staggering. So staggering it matches dollar for dollar the amount of money spent online buying and selling stuff.

The ransomware attack in May 2017 called Wannacry caused $8billion of damage and over 300,000 business computers were infected.

Last year, the financial services industry was worst hit followed by utilities and energy and then technology companies, where between them, they lost $42billion overall before security costs.

By 2019, the nearest estimates from the cyber-security industry is that $1 trillion will have to be spent defending the $2 trillion of expected losses.

You would be forgiven for thinking that humanity is attacking itself and that none of us are ever going to be immune from such a devastating event as identity theft and you're probably right. And yet, there's a strange number that has just emerged.

A survey just out, sponsored by Opus and conducted by Ponemon Institute, shows 67% of Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) believe their companies will likely fall victim to a cyberattack or data breach in 2018. And incredibly, 60% are concerned that a partner or vendor will be to blame.

The most threatening factors named by CISOs, in this order, are:

- The human factor (70% cited "lack of competent in-house staff")
- Inadequate in-house expertise (cited by 65% of respondents)
- Careless employee falling for a phishing scam (65% chance)
- A malware attack, a data breach or a cyberattack (unspecified percentage)
- Inability to protect sensitive and confidential data from unauthorized access (59%)
- Inability to keep up with the sophistication of the attackers (56%)
- Failure to control third parties' use of sensitive data (51%.)
- Disruptive technologies – i.e. Internet of Things (IoT) devices (60% of respondents considered these the most challenging to secure)
- Mobile (54%)
- Cloud (50%)

In other words, the first three on this list are one and the same – that is – human error. The fact that another 60 percent of security officers expect malware, hack attacks and the like to cause a serious data breach, is itself an alarming number.

According to the same poll, less than half of the security officers surveyed believe their IT security budgets will increase, yet the threat of losses over the course of just one year is likely to increase many times over.

The rapid escalation of targeted cyber-attacks is no longer surprising news. In 2016 an outfit named 'shadowbrokers' breached the spy tools of the elite NSA-linked operation known as the Equation Group and caused havoc as they were made up of malware, viruses, trojans, weaponised 'zero day' exploits and remote control systems – all designed by government to spy on or cause disruption to citizens. Let's not forget what this really means. Nation-state cyber weapons are now in the hands of criminals.

In 2017, the voter records of just about every American registered to vote for the last ten years was hacked and presidential candidates had their servers attacked and incriminating email distributed on every continent in the world.

In the meantime, the online cyber-threats to you personally are changing shape. Socially engineered malware now led by data-encrypting ransomware, provides the No. 1 method of attack. Password 'phishing' attacks are next, un-patched software, social media hacks and 'spear-phishing' bring up the rear. These are all known as 'advanced persistent threats' for good reason.

Sky News has just reported that a "text bomb" has been discovered which can crash iPhones just by being sent to a victim's device.

Software developer Abraham Masri discovered the bug and said he released it to get Apple's attention after his reports and warning to the company went unheeded. The "text bomb" code is so toxic for iPhones that devices which were sent a link to the code would also crash – even if they didn't actually click the link.

With the arrival of cyberwarfare, every device has now become a battlefield of sorts. If you didn't know already, cyberwarfare is the use of digital attacks by one country to completely disrupt the computer systems of another with the aim of creating significant harm, death and destruction. Future wars will now be fought not just by new weapons but by hackers using computer code to attack an enemy's infrastructure.

In addition, a new project called the Computational Propaganda Research Project (COMPROP) has identified how organisations, often with public money, have created a system to help '*define and manage what is in the best interest of the public*.' In reality the analysis shows how political parties and governments use tools like social media bots to manipulate public opinion by amplifying or repressing political content, disinformation, hate speech, junk or fake news. In the west, The US and UK governments top that list.

Modern western economies, are underpinned by computer networks that run everything from communication systems, food and water distribution to food supply chains. As we have already seen, governments are woefully prepared and therefore are particularly vulnerable to such attacks. But with continued and ever more damaging attacks, cyberattacks and cyber-warfare will rapidly rise close to the top of the political threat agendas of governments all over the world in the next two or three years. But let's not forget the ineptitude of employees or contractors.

A nuclear power plant in Germany was infected with malware as the result of employees bringing in USB flash drives from the outside. And malware was found in the control room of a Japanese nuclear reactor.

ZDNet reports that "The head of the US National Security Agency (NSA) Admiral Michael Rogers said his worst case cyberattack scenario would involve "outright destructive attacks", focused on some aspects of critical US infrastructure and coupled with data manipulation "on a massive scale". Shutting down the power supply or scrambling bank records could easily do major damage to any economy. And some experts warn it's a case of when, not if."

It looks like Warren Buffett was right – technology is already becoming the new number one threat to mankind.

*

Featured image is from TruePublica.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: True Publica