CYBERSECURITY HAS FAILED: WE NEED A NEW PARADIGM

CO-AUTHORS:

Jack B. Blount
President & CEO
Intrusion Inc.

Bob Barker
Founder and CEO
The Partnering Network

*Previously published on advisenltd.com
The common vulnerabilities and exploits (CVE) database lists more than 11,000 exploitable vulnerabilities in commonly used systems and software — and as of mid-2019, 34 percent had no patches available.

- JOSH FRUHLINGER, CSO, MARCH 9, 2020
HOW CYBERSECURITY IS FAILING

The threat of cyberattacks to businesses worldwide has become immense and continues to grow. While significant measures have been taken to address this acceleration of cyber aggression, the figures remain mind-numbing.
KEY CYBERSECURITY STATISTICS AT-A-GLANCE

- **94 PERCENT** of malware is delivered via email.
- Phishing attacks account for **more than 80 PERCENT** of reported security incidents.
- **$17,700** is lost every minute due to phishing attacks.
- **60 PERCENT** of breaches involved vulnerabilities for which a patch was available but not applied.
- **63 PERCENT** of companies said their data was potentially compromised within the last twelve months due to a hardware- or silicon-level security breach.
KEY CYBERSECURITY STATISTICS AT-A-GLANCE

- Attacks on IoT devices \textbf{tripled} in the first half of 2019.
- Fileless attacks grew by \textbf{256 percent} over the first half of 2019.
- Data breaches cost enterprises an average of \textbf{$3.92\text{ million}}.
- 40 percent of IT leaders say cybersecurity jobs are the most difficult to fill.
A DELL SURVEY REVEALED THAT

63% OF COMPANIES IDENTIFIED A HARDWARE-LEVEL OR SILICON-LEVEL SECURITY BREACH AS THE REASON THEIR DATA WAS COMPROMISED WITHIN THE LAST TWELVE MONTHS
CYBERSECURITY VENTURES PREDICTS GLOBAL SPENDING ON CYBERSECURITY PRODUCTS AND SERVICES WILL EXCEED $1 TRILLION CUMULATIVELY OVER THE FIVE-YEAR PERIOD FROM 2017 TO 2021.
THE CYBERSECURITY INDUSTRY AS A WHOLE IS FAILING TO PROTECT OUR ECONOMY

IT’S TIME TO FIND A NEW PARADIGM THAT IS BASED ON AN ENHANCED ARCHITECTURE. TO ACCOMPLISH THIS, WE WILL:

1. Examine the nature of cyber threats, then review their impact on large and small businesses;
2. Expose current false assumptions that prevent dealing in a realistic way with a cyber problem far greater than even most cyber professionals recognize; and
3. Define new assumptions and a new, more realistic paradigm that is needed to enable progress and make the world safer from cybercrime and cyber warfare.
THE NATURE OF CYBER THREATS

CYBERCRIME

The use of computers to execute crime against a person, business, or other entity through digital attacks on a network, computer, or an account to gain profit or cause chaos, damage, or confusion.

VS

CYBER WARFARE

In contrast, cyber warfare refers specifically to the use of digital attacks by foreign nations to damage the networks and computer systems of another nation or to create chaos or confusion.
MOST BUSINESSES IN AMERICA HAVE BEEN BREACHED BUT DO NOT REPORT IT FOR FEAR OF DAMAGING THEIR REPUTATION.
## CHANGING THE PARADIGM

<table>
<thead>
<tr>
<th>LARGE ENTERPRISES AND GOVERNMENT</th>
<th>SMALL AND MEDIUM ENTERPRISES</th>
</tr>
</thead>
<tbody>
<tr>
<td>A common assumption among CISOs is “you haven’t been breached if you don’t know it,” and that is simply untrue. Sony, the FBI, The Home Depot, JP Morgan Chase, and the other millions of businesses that got breached will tell you they did not know of their breaches until it was too late. Almost every business – no matter how large or small – has been breached. Agents are living on your network, examining what data you have, and searching for what’s most valuable to them.</td>
<td>According to the SBA, more than 30 million small businesses exist in the U.S., employing almost half the private workforce. Cyberattacks are an even greater danger to small and medium businesses because according to the FBI, 60 percent of businesses that experience a ransomware breach fail soon thereafter.</td>
</tr>
</tbody>
</table>
If firewalls stay updated, the network stays protected.

Software and hardware from trusted vendors is secure when delivered.

An intrusion protection system or DNS tool will spot the bad guys and keep the network safe.

The right number of people with the right talent will keep the network safe.
ELEMENTS OF A NEW PARADIGM

To replace the current, unrealistically positive view of cyber resilience with a new, realistic paradigm means starting from a very different perspective. Here are the key components of such a paradigm that CISOs and other IT professionals must adopt if they are to have a fighting chance of protecting their company’s valuable data:
Accept that you can’t keep the bad actors out of your network. Large company and small company CISOs need to be aware of this fact and not be complacent.

Similarly to the acceptance that bad actors will enter your network, you must operate on the belief that everything in your network has already been compromised.
Once you’ve adjusted your mindset, the focus should shift to finding ways to neutralize threats while they’re on your network.

Look for and employ solutions that eliminate the unrealistic volume of false positives, making it more practical for your personnel to address the real threats.
IMPLEMENTING A NEW PARADIGM

INTRUSION has created a services solution for businesses that acknowledges these realities. INTRUSION Shield™ is based upon the premise that all networks are compromised from malware embedded in foreign manufactured device components, breaches of firewalls, memory sticks, IoT devices, and dozens of other methods.
INTRUSION SHIELD™ IS A NEW PARADIGM AND A NEXT-GENERATION CYBERSECURITY SOLUTION THAT IS REAL-TIME, LOW COST, EASY TO USE, UPDATED DAILY AND PROVIDES BOTH IT AND BOARD-LEVEL TRANSPARENCY TO ALL NETWORK ACTIVITY.
TO LEARN MORE

Contact us today to learn more and to see if you qualify for a free trial that requires no displacement of your existing infrastructure.

REACH OUT TO US AT (888) 637-7770
OR INFO@INTRUSION.COM.