The Need for a Breakthrough in Cybersecurity

By: Ricardo Villadiego

Table of Contents

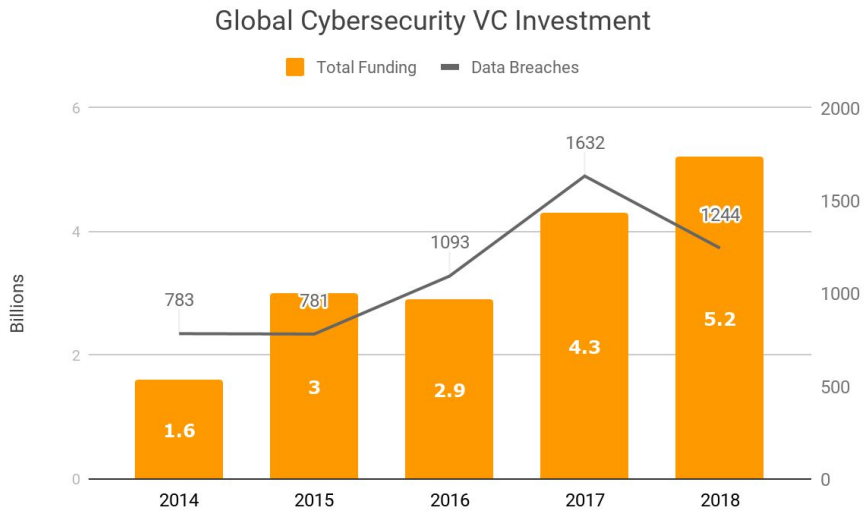
Executive Summary

This document compares the level of venture capital (VC) investment in the cybersecurity industry with the reported breaches in the United States. The conclusion of this comparison encourages security professionals to explore the reasons why the cybersecurity industry is underperforming from the protection point of view, despite the level of investment. This document assesses the reactive nature of the industry, the complexity in the decision-making process, and the subsequent consequences for the organization. The lack of a feedback loop in current cybersecurity architectures is also examined. Lastly, the paper discusses the breakthrough of a cybersecurity concept denominated **continuous compromise assessment**, which implements a much needed feedback loop into enterprises' security architectures.

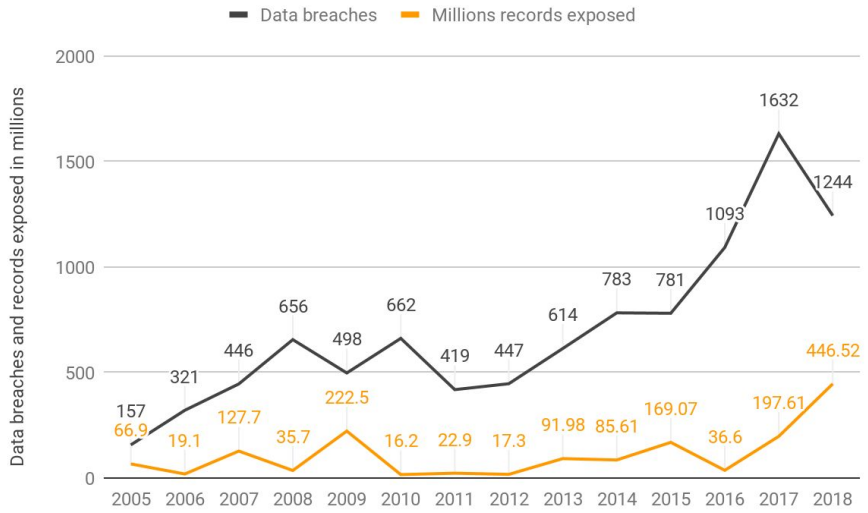
The State of Cybersecurity

The cybersecurity industry is sizzling. For starters, VCs continue to deploy unprecedented capital to enable the growth of existing vendors and fund new ones. Between 2014 and 2018, the VC industry deployed an astonishing $17.1 Billion, according to strategic cyber ventures[1].

Between 2014 and 2018, the VC industry deployed an astonishing $17.1 Billion



Yet, during the same time period, the number of security breaches increased exponentially, and the amount of exposed data resulted in a crisis of global scale. According to the U.S. Identity Theft Resource Center[2], the number of breaches grew from 783 in 2014, an already frightening number, to a peak of 1632 in 2017.



[1] 2018 Cybersecurity Venture Capital Investment: https://scvgroup.net/2018-cybersecurity-venture-capital-investment/
[2] 2018 Identity Theft Resource Center 2018 Data Breach Report

The same study reflects that the problem is widely spread across all industries.

Number of U.S. data breach

Year	Banking/ Credit/ Financial	Business	Educational	Government/ Military	Medical/ Healthcare	Total
2013	35	194	54	60	271	614
2014	38	263	57	91	332	781
2015	71	312	58	63	275	779
2016	51	497	97	72	373	1090
2017	134	907	128	79	384	1632
2018	135	572	77	100	367	1251

Investment does not necessarily translate to protection

It is untrue that organizations that adhere to the most stringent regulatory standards - such as in the banking sector - perform better than others that are less regulated, or that industries that invest heavily in cybersecurity are less breached. It is probably time to accept that investment does not necessarily translate to protection.

For years, we have been conditioned to define success in terms of the investment of time and money. In cybersecurity, this well-proven formula is not producing the results we should expect to see from an industry that has such a high level of investment.

That universal formula (Success = Time + Money) has worked in most aspects of life, from sports to sending a man to the moon. That same formula is producing impressive results in the health field. In August of 2019, the WHO and the National Institute of Allergies and Infectious Diseases announced a cure for Ebola, and significant progress has been made towards an HIV vaccine, a disease that meant death about 20 years ago.

However, the cybersecurity outlook is disappointing, and the cyber-war may be lost. Another indication of this is an iconic brand like Capital One announcing being a victim of a massive breach. How we arrived to this point deserves exploration.

How Did We Get Here?

There are four main drivers that led the industry to its current state of compromise and uncertainty:

a. **Ever-evolving threats** generate an infinite number of vulnerabilities that enterprises must attempt to defend. Cybersecurity technologies continue to be mostly reactive which leads to a vicious "cyber cycle" of attackers scanning networks, developing exploits and attacking systems, with defenders detecting attacks, analyzing exploits and patching such systems.

b. **Unlimited capital** flowing into the industry is fueling defense vendors that fall into the "detect then mitigate" approach. The results are technologies in-market that are not ready for primetime, inherently unstable and becoming obsolete as soon as deployments are completed without ever testing if they delivered on their promise.

c. As a result of a.) and b.), cyber-defense architectures have **grown in complexity**, stacking an avalanche of vendors that neglected management and monitoring capabilities, hence adding little incremental protection to the system. The complexity and cost associated with it create a false sense of security, especially at higher levels in the organization.

d. Today's society is psychologically wired to find instant gratification. This notion is translated to problem-solving as the pursuit of **the magical solution** ("the silver bullet"). This behavior and the inability to embrace the idea of being breached led practitioners and decision-makers to accept the current framework of innovation in cybersecurity: detect then mitigate.

The complexity and cost associated with it create a false sense of security

To make matters worse, many of today's cybersecurity solutions and architectures work as an open-loop system at their core. This means systems do not take into account the redeeming features of closed-loop systems, in which the ideal output (in this case the state of no compromise) is measured continuously to make sure that changes are applied to the system (the cybersecurity architecture).

It's impossible to obtain different results doing more of the same. In order to break the cyber cycle, cybersecurity needs to make a fundamental shift towards applying control theory to continuously measure the value of reference. For a given organization, it must be **"no compromise."** Any deviation from the reference value should be promptly identified and mitigated by adjusting the cyber defense architecture.

Making the Right Decisions

Organizations must decide on the right defense strategy for their business model, industry and stakeholders. This means maintaining an efficient, effective, and proactive approach while keeping reduction of failover rates in check. However, in light of the significant increase in breaches over the last decade, are we making the right decisions?

A recent[3] study stated that the challenges of building cybersecurity capabilities in organizations are rooted in misconceptions about two particular aspects of complexity that have received little attention:

If a company does not experience any cyberattacks—more precisely, if it does not detect any cyberattacks—there is little motivation to invest in cybersecurity

- **The uncertainty surrounding cyber incidents:** Security and risk professionals find it difficult to apply conventional decision-making theories to cybersecurity investments due to the difficulty of measuring the impact of a hypothetical cyber incident. Consequently, they often make decisions and judgements based on their experience and their best knowledge concerning the likelihood of uncertain events.

  The uncertain nature and severity of cyber threats, combined with frequent shifts in technology acquisition and the introduction of new vulnerabilities makes it difficult for decision makers to efficiently allocate resources for investment in cybersecurity capabilities. The growing presence of cyber threats has created an environment that focuses on technical defenses but neglects the economics of cybersecurity investment. If a company does not experience any cyberattacks—more precisely, if it does not detect any cyberattacks—there is little motivation to invest in cybersecurity. For this reason, many industry professionals often do not envision cyber risks properly. It is not surprising to observe significant gaps between perceptions and the actual state of the cybersecurity of their organizations. As a result, they may underestimate the frequency in which incidents occur, and the time it takes for cybersecurity solutions to start working, preventing, detecting, and responding to an incident.

- **Delays in building cybersecurity capabilities:** Cybersecurity has grown in complexity, and it will likely continue to do so. As other complex models, cybersecurity systems include potential delays. In a reactive organization in which managers start investing in the development of cybersecurity capabilities only after detecting an attack, the organization's computer-based information systems will not properly recover on time and will remain vulnerable. As King Henry VIII from England once said: "Of all losses, time is the most irrecuperable for it can never be redeemed." If organizations could avoid this reactive approach, fight the urge of falling into the trap of short-termism, and act decisively to implement the cybersecurity capabilities that they require, they would be in a better position.

[3] Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment.

The Cybersecurity Breakthrough

The global cybersecurity crisis is a problem that must be solved, or significantly improved in the short term. VCs are rightfully continuing to deploy capital in the industry. With a threat landscape that can and will evolve infinitely, addressing the problem is ever more critical.

Organizations have to assume that cybercriminals are already inside

The focus must be placed in building cybersecurity capabilities that fundamentally disrupt the current state of cybersecurity. We need to rethink our security paradigm from the long-standing one of trying to keep adversaries out of our networks. Organizations have to assume that cybercriminals are already inside. This is known in government circles as "Assumption of Breach." Deborah Hayden of the NSA's Information Assurance Directorate has said as much back in December, 2010.[4]

The industry lacks a factual process that provides certainty around cyber incidents, which is one of the two drivers for making the right cybersecurity decisions. At Lumu, we call this process ***continuous compromise assessment***.

To better understand this concept, it is necessary to first revise the Cyber Kill Chain[5], which is a model for the identification and prevention of cyber intrusions activity. The model identifies what adversaries must complete in order to achieve the objective. The following is a simplified graph of the process.

A closer look at the different stages among the multiple variations of the Cyber Kill Chain unveils the common denominator that enables adversaries evil intent: **network access**. Network traffic is ground zero for illuminating threats. Almost all threats must first be downloaded and then communicate back to its C&C to provide any value to attackers.

The ability to collect network traffic to illuminate threats may be the **feedback loop** that many cybersecurity and academic researchers have been envisioning for over a decade.

The ability to collect network traffic to illuminate threats may be the **feedback loop** that many cybersecurity and academic researchers have been envisioning for over a decade

Even with the advances in bandwidth and storage, collecting network traffic for a large organization might be cost-prohibitive. The problem now evolves into how to collect signals of network traffic in a way that accurately represents the summary of the “conversations” within an organization.

[4] Assumption of Breach: The New Security Paradigm by Jeffrey Carr
[5] Developed by Lockheed Martin
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

In his book *Secrets and Lies*, Bruce Schneier formulates "that often the patterns of communications are just as important as the content of the communication." For example, the simple fact that Alice telephones a known terrorist every week is more important than the details of their conversation. Putting this together with the steps associated with the Cyber Kill Chain, we can quickly realize that the process of compromising a device and a network will make that device and network behave differently. Here are a few steps to illustrate the process:

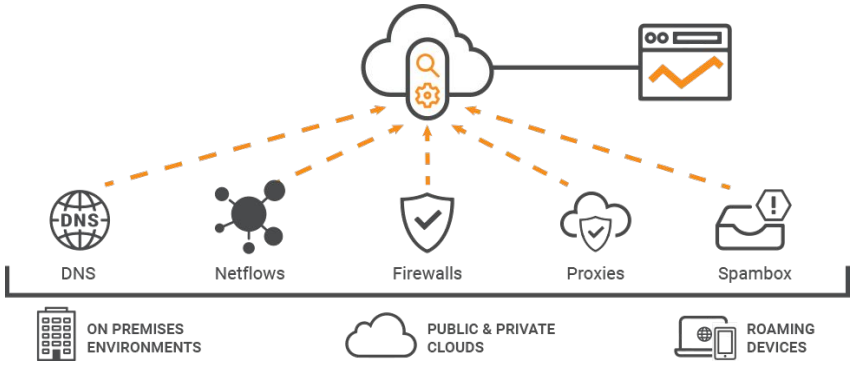
- The end-user who the adversary is targeting will point his or her device to a new **host**.
- If the attack is successful, the device will attempt to connect with the adversary's infrastructure **(C&C)** seeking instructions and/or exfiltrating information.
- In more sophisticated attacks, the adversary will need to escalate privileges and, in order to do so, the compromised device will attempt communications with adjacent devices and/or high-value targets within the now compromised organization. This is a clear sign of **lateral movement**.
- As the adversary conquers new victims, more devices will attempt to connect with the adversary's infrastructure.

Further analysis of the described steps among many others facilitated the key elements of metadata, from required network traffic to an accurate representation the summary of conversations within an organization, as described in the following table:

Network Metadata	Why it Matters
DNS Queries	Collecting DNS Queries provides context into the attempt of connections from the organization's devices towards adversarial infrastructure.
Network Flows	Among other malicious behavior, network flows provide insights into an organization's devices that are controlled by the adversaries and attempt to move laterally.
Access Logs of Perimeter Proxies or Firewalls	In cases where the attacks avoid domain resolution, the traces of adversarial contact will lie in the access log of firewalls or proxies, depending on the organization's network configuration.
Spambox	Email is the preferred method by attackers to deliver exploits to the organization's end-users[6]. Analyzing the organization's spambox provide insights into the type of attacks an organization is receiving, but more importantly if end-users are accessing such attacks and the organization is at a high risk of compromise.

[6] Verizon 2019 Data Breach Report.

Signaling traffic in this form instead of doing a full packet capture is optimal, as it represents only a tiny fraction of the total network traffic. Yet it's still possible to identify the compromise level of an organization.



Specific techniques have been developed to facilitate the data collection process while minimizing friction in the multiple environments that define a network nowadays.

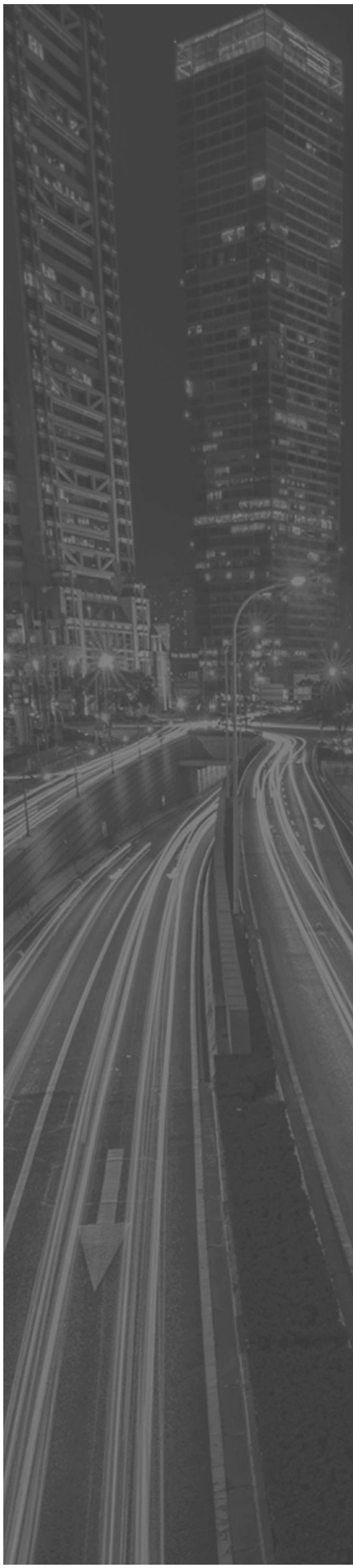
The remaining problem to solve is how to make it a continuous process. Collecting and processing these signals for a specific timespan is feasible, but it is challenging. Organizations can quickly become disenchanted due to the level of complexity in data collection and processing, even using tools that promise to handle at least some of these key signals, like SIEMs or network flow collectors.

To solve this last piece, a reliable, accurate and continuous process is required from collection to Illumination as shown in the following image.

Only once the continuous process is implemented can we say that the feedback loop has been built and this can be considered the breakthrough for cybersecurity in modern days. A continuous compromise assessment process will not only simplify the decision-making process for managers and practitioners but will also entirely change the dynamics of the cybersecurity ecosystem and the cyber cycle of attackers versus defenders.

Conclusion

Cybersecurity is complex. Success in complex scenarios lies in the system's ability to regulate from disturbances. In practice, this is done via closed-loop systems or "error-controlled systems" defining error as the state of compromise for a particular cybersecurity incident. The faster the industry moves towards developing the necessary cybersecurity capabilities that help an organization assess its continuous status of compromise, the faster that cyber-resilience will be achieved. With small but deliberate changes to the cyber-security architecture, the disparity between the cyber incident and the detection of the breach can be dramatically shortened.



Illuminating threats and adversaries

www.lumu.io

Lumu Technologies Inc. | 8350 NW 52nd Terrace Suite 301, Miami, FL 33166 | info@lumu.io | +1 (877) 909-5868