THE CHANGING CYBER THREAT ENVIRONMENT

Discussion with Aron Szekely, Cyber Security Adviser, ERG Partners

With endless high profile attacks and skyrocketing cost of malware attacks and cybercrime, awareness of cyber risk among organizations has increased and cyber security has become a key board level concern. However, the cyber risk environment is changing and threats are evolving. While large corporate and government agencies tended to be the primary target, malicious actors are increasingly targeting a broader set of potential victims. Most recently, the closure of offices and the necessity of working from home resulting from COVID-19 and the reliance on video conferencing have created new vulnerabilities.

In order to understand the changing landscape we sat down with **Áron Székely**, a cyber security adviser to ERG Partners, who has advised major financial institutions, global corporations and smaller companies on cyber security and how to protect themselves and their infrastructure against evolving threats.

Attacking is always cheaper than defending – Here are some counter strategies

Áron - Thanks for taking the time to sit down with us. You speak with clients about the threats they are facing on a daily basis, and have a global view on the cyber threat environment. Can you talk about how the risk environment is changing?

Áron Székely
ERG Partners Cyber Adviser

Thank you for having me. Risk to enterprises, small and large, is increasing globally. This is due to a multitude of factors. The expression 'software is eating the world' has been in use for a few years now, and unfortunately, where there is software, there will be vulnerabilities, and where there are vulnerabilities, there will be actors who will try to exploit them for financial or strategic gain.

A fundamental issue is that attacking is always easier and cheaper than defending, and it is easy for an adversary with few resources to find victims using commodity tools that are often in use in legitimate computing. It is virtually the same effort to scan 5 or 5000 potential victims, and even one successful attack can yield serious gains. Another problem is that attackers can do more with data that they find online. They may use personal information themselves, or sell it for further malicious activity, such as identity theft, etc. It is also easier to aggregate and correlate data from various sources and build up intelligence on high value targets, which with the right planning result is a serious prize for the attackers.

Attacking is always cheaper than defending

The advent of cloud computing is a double edged sword: on one hand, it is alleviating a lot of risk by taking serious tasks off users' endpoints and making it possible for competent service providers to provide better security by leveraging economies of scale. On the other hand, the shared responsibility model of cloud computing is often misunderstood by both companies that build their product on cloud platforms, as well as end users: misconfigurations, bugs in software, gaps in process, etc. are not within the purview of the cloud provider, and companies still need competent staff with domain knowledge in order to provide secure and reliable services. Data breaches such as ones stemming

from public S3 storage buckets on AWS, or unauthenticated databases reachable via the public Internet highlight this painful gap.

Lastly, the prevalence of mobile devices is creating an ever increasing attack surface with the advent of Bring Your Own Device (BYOD) in a lot of workplaces. The complexity created by BYOD increases the complexity of securing firm data. We also have seen a rather significant rise in attacks targeting mobile devices as attackers are discovering and attempting to exploit an area that is still rife with vulnerabilities.

COVID-19 and near universal social distancing and working from home has introduced new vulnerabilities. For example, Zoom, and other video conference platforms, which individuals and organizations are using while offices remain closed, expose users to new risks. Can you discuss what these are?

Traditionally, we used to think that if we protect the perimeter of our computing environment by surrounding it with firewalls and intrusion detection systems, we improved our risk posture. Unfortunately, due to mobile computing and an organization's network extending virtually indefinitely, blurring the perimeter, this model is no longer tenable. VPNs and remote access software open up an organization's network to threats via the user's endpoint devices, simply in order for users to be able to get their work done. Building secure remote access solutions can take years, and in the wake of the COVID-19 pandemic, organizations had to scramble to provide connectivity in a matter of a few days, at most weeks. On top of the lack of time, a lot of enterprises have neither the funds, nor the expertise to provide a secure solution for their workers, and resort to free or cheap tools.

Data leakage and theft through infected or hijacked endpoints is a major risk, but even something as trivial as an attacker stealthily joining an unauthenticated Zoom video conferencing session and being privy to confidential firm information is in itself a threat. Legitimate users recording teleconferencing sessions without an understanding of what happens with the recorded video can end up with putting company information on the public Internet for anyone to download. Furthermore, the software used for remote access and remote communications itself can have bugs that can be exploited. It is extremely important for companies to do their due diligence when selecting vendors for remote work to have at least some access control in place, and also to have incident response procedures in case of a breach. I should add here that not all controls that decrease risk need to be technical. A lot can be accomplished at a lower cost by having the right business procedures in place as well as user education.

This last element of end-user education is exceptionally important as we see more and more COVID-19 themed phishing emails, with lures that relate to medical equipment, or cures for the virus. Scams targeted at individuals exploiting users' psychological uncertainty are one aspect of this, an even more dangerous one is ransomware targeting hospitals, potentially leading to even loss of lives.

Where there are vulnerabilities, there will be actors who will try to exploit them

We also see a notable increase in payment card fraud and digital skimming, since most shopping is moving online during the pandemic. Threat actors benefit from slower response time and impaired operations in most places' IT and security departments. One particularly high yield scenario for attackers is to compromise employees working from home that have higher privileges to certain services. For example, taking control of a customer service representative's machine could expose customer data and can then be used as a pivot point into other firm systems. Employees of managed service providers (MSPs), companies who provide IT services should be particularly careful, since a compromise in their systems puts all their customers at risk.

What can organizations do to manage their cyber risks and prevent attacks that jeopardize their businesses? Particularly in light of the changes you described, what can smaller organizations such as private equity funds, family offices, and entrepreneurs-led businesses do?

It is an uncomfortable truth that nobody is 100% safe in cyberspace, especially not from well-funded attackers such as state sponsored actors. If an adversary is well funded enough, they will breach your defenses and get what they want. Defending against cyber attackers is in large part a mathematical game of who can keep up the battle longer. If we, as defenders manage to raise the bar high enough that attackers exhaust their resources, they will move on to easier targets. There are a number of measures that can be taken to accomplish this.

The first thing every organization should do is to catalogue its assets and identify what the highest value targets are for malicious parties. This analysis can be combined with the development of a BCP/DR (Business Continuity Planning/Disaster Recovery) procedures, since it is highly likely that these are the core assets that allow the business to function. It is important to keep in mind that the goal is to maximize the ROI on our investment into security, so we should make decisions that optimize cost vs. decrease in risk. Once we identify key assets, we can focus on limiting access to those,

making sure to take into account not only external factors but also the possibility of insider threat.

It is an uncomfortable truth that nobody is 100% safe in cyberspace

Another important yet often overlooked aspect of successful defense is an accurate inventory of the organizations' IT components. This includes endpoints, servers, and even Sofware-as-a-Service accounts. Not having an accurate inventory can lead to what is commonly called 'Shadow IT', which means that an organization does not have 100% visibility on its IT infrastructure. Lack of visibility represents a huge business risk. Fortunately, there are quite a few vendors out there providing services that include the ability to construct and maintain an accurate and up-to-date asset inventory.

BCP/DR procedures mentioned above as well as security and other IT incident response procedures being in place is another key factor that differentiates mature organizations. Having regular DR testing and Incident Response testing at frequent intervals can help not only to satisfy audits and regulatory requirements, but also makes sure that the organization is constantly improving itself and adapting to changes within its own business and technical environment. A well-documented and rigorous, preferably automated, change management process is also a huge asset in an organization's security posture.

I need to emphasize the importance of users again here. Sophisticated technical controls and optimized procedures mean nothing if your users do not cooperate and are looking for ways to circumvent the controls in place. Security within the enterprise is a game where the goalposts are constantly shifting and a mindset of 'set it and forget it' will almost certainly lead to catastrophic failure. Organizations must constantly weigh trade-offs between security and usability. It is surprising how much inconvenience users are willing to put up with if the reasons for these measures are communicated to them clearly. If your users understand why your security controls are in place, they no longer perceive them as a bunch of unnecessary hoops they need to jump through.

A key problem seems to be that in many cases the intrusion may have happened months before the victim organization detects it, and at that point controlling the damage caused by the attack is difficult if not too late. How can organizations ensure that they detect malware attacks as quickly as possible to minimize the cost and damage?

Based on past experience this is an area where I cannot be too optimistic, since dwell time for adversaries in an organization's systems is usually quite high. This does not mean that there aren't measures that can be taken: carefully auditing access to key business information and putting in a detection system, preferably automated, for anomalies goes a long way. In general, establishing consistent baselines of what normal usage means will help identify any unauthorized access. Unusual network traffic, users accessing information at odd hours, or too many failed attempts accessing privileged data can all be indicators of compromised systems. Regular BCP/DR and Incident Response exercises are a great way to make sure that you can minimize both financial as well as reputational damage.

There are common technical controls that can be put in place, a lot of vendors offer comprehensive suites that include endpoint protection, spam filtering, traffic filtering, etc...but I cannot emphasize enough the importance of user education and regular training exercises. Creating and maintaining security awareness amidst users can lead to employees reporting observed anomalous activity. As a proactive measure, you can subscribe to free and paid online resources to see if your organization's data appears in publicly available dumps resulting from compromise.

Where there is software, there will be vulnerabilities

Regular updating and patching of IT systems, endpoints and server infrastructure, is a non-negotiable component of a mature organization. Where possible, organizations should leverage automation in their architecture to perform proactive vulnerability scanning of systems before they are launched, and not let anything go into a live production environment that has known security holes. Organizations should conduct regular scans of their whole infrastructure, especially as

vulnerabilities are uncovered daily. Where possible, architect for high availability and make changes to your infrastructure in a way that prevents adversaries from dwelling by simply destroying and recreating infrastructure. Servers or endpoints that are re-imaged from scratch periodically make it more difficult for adversaries to hide in your network for a long time.

Lastly, heavy emphasis should be placed on protecting high value business targets such as executives, and building a profile of normal activity on their behalf. Unfortunately Business Email Compromise (BEC) has led to millions of dollars in losses in the last few years, so IT and Security teams should exercise maximum diligence in protecting high ranking members of an organization.

How can smaller organizations with limited IT resources afford and execute these strategies?

Great question. I am a firm advocate of small organizations moving a lot of their infrastructure into the

cloud where they benefit from the scale and experience of SaaS providers. Asset inventories, and identity and privilege management are made simpler and easier due to most providers exposing APIs to automate daily operations. The monthly cost is surprisingly reasonable when broken down to a per user per month price tag. Initial setup and integration can be done with an outside security consulting company, and one can sign up for a maintenance contract or periodic review for a sum that won't break the bank.

If there is an attack what can and should organizations do and how? What are the key risk factors?

This will vary based on the line of business that you are in, but it is key to have an incident response procedure that when activated is not only technical in nature but also describes the communications aspect of things. During a breach, how do you communicate safely and effectively within the company, throughout your chain of command. Once you recover, how do you notify your customers, and if necessary, the authorities, plus any regulatory bodies? Companies that have rehearsed these scenarios will have a clear advantage. Once you have the process down to a T, you can think about automating it.

In general organizations should follow the standard procedure of Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. There is no one-size-fits-all solution in implementing the process, but it is key to keep in mind the last phase where you review your incident and improve your process: as mentioned before, organizations need to constantly improve their security practices and procedures. Cybersecurity is a never-ending race.

Companies that do not have direct access to client or personal data can unfortunately still present a risk. For example, compromising one of your business email accounts may not yield any immediate gain, but using that email account to send malicious links to every one of your clients has a high potential to succeed, since your clients are more likely to open attachments from you, a trusted party. I should add, that no matter how small your company, or how limited your exposure to confidential data, the best solution in my opinion is to responsibly disclose any breach to your clients and partners as soon as possible. This can make a huge difference in terms of malicious actors gaining more footholds into other businesses.

It appears that geopolitical tensions are increasing cyber operations by state sponsored adversaries, for reasons ranging from traditional intelligence gathering to further their geostrategic goals and malicious activity targeting dissidents and minority populations to IP theft and industrial espionage in support of their domestic industries, and counteracting the effects of international sanctions. What do you see happening in the state sponsored actor there?

Unfortunately state sponsored actors are the hardest ones to protect against. They effectively have an inexhaustible set of resources and a very deep bench of malicious talent. Certain rogue states even rely on cybercrime for funding themselves. The situation in that space is only going to get more heated, since, as I mentioned earlier, attacking is cheap, defense is expensive and difficult, and the barrier to entry is low, promising high political and financial gains. The rules of attacker math dictate that it is extremely difficult to protect against an adversary who has a virtually inexhaustible pool of resources.

The Internet by default was not designed with security in mind, yet more and more devices become connected, so the attack surface will only keep growing. As more and more critical aspects of our lives move onto the Internet, protecting critical infrastructure should be number one priority in every country, and for every government. This requires action on the national as well as the international level, and a close cooperation between the public and private sectors.

-

Áron, many thanks for your insights.

CONTACT ERG PARTNERS

If you have any questions regarding the issues discussed above, require additional information or would like to schedule a meeting to discuss the requirements of your organization and how ERG partners could assist, please contact one of the following individuals at **ERG Partners**:

Tapio Vaskio
Managing Director
+1 646 552 4038
tvaskio@ergpartners.com

Arpad Krizsan
Managing Director
+1 646 250 8634
akrizsan@ergpartners.com

Aron Szekely
Cyber Security Adviser
+1 347 301-1874
aszekely@ergpartners.com