3

State of the Art – How and Why?

Palo Alto Networks – Greg Day, Vice President and Regional Chief Security Officer, Europe, Middle East and Africa

- Intelligence on cyber threats is key
- Be sure your cybersecurity is built on a solid foundation
- Multiple legacy technologies create inefficiencies—clear out the deadwood
- Cybersecurity should enable the business, not inhibit it
- Aim for more systemic success

'State of the art' is now a key term in new EU cybersecurity legislation—and outdated cyber capabilities could leave your business unnecessarily exposed to risk.

As our dependencies on technology grow, new EU legislation has introduced the term 'state of the art' into our vocabulary, as a part of the security by design and default concept in the General Data Protection Regulation. The term is also used in the Network and Information Security Directive, which is focused on the cybersecurity of essential services and digital services provision. Such a simple term will have significant impact on your business in the future, so it's worth considering now what it means to your business and others (such as auditors, customers, and partners).

On first glance, this may seem both easy and confusing, depending on your background. Those in financial services have been used to more prescriptive requirements from their own regulators, while others may look at this term as exactly what they, as security teams, do every single day: to continue to monitor the risk and adapt their cybersecurity capabilities to manage their risk. In many ways,

the latter is why it is now the time to step back and consider what 'state of the art' really means.

You may consider this as detail, but here is why you should care and ask questions of your cybersecurity team: outdated cyber capabilities will leave your business unnecessarily exposed to risk, may cost you more to manage, and could lead to significant, unnecessary commercial impact.

In today's technology-driven world, the pace of change is relentless; as such, cybersecurity must continue to adapt to changing technology, new threats, and evolving business practices. In the 30 years I have spent working in the cybersecurity industry, the pace has never eased. Every year we have new problems to solve while we simultaneously try to consolidate existing capabilities. This creates a fundamental challenge: as we keep evolving, we never step back to look at the big picture. Are the cybersecurity fundamentals we started with so many years ago still sound today? For centuries we believed the world was flat, until science proved otherwise. Are our cybersecurity capabilities limited by similar, outdated beliefs?

So what are some of the principles that need to change?

1. Just as in every other aspect of business, intelligence is key. There is an ever-increasing number of cyber 'things' that could happen—the crucial questions are, "Which are most likely?" and "Which would have the most significant impact?" Validating this means not only leveraging commercial sources but also connecting to the right industry knowledge and sharing groups and effectively leveraging your own organic intelligence. The new legislation talks about 'having regard to' or 'taking into account' the state of the art, which could mean that you should be able to show you have current insight on what the threats are and how they could impact your business and your customers. You need to challenge your team to confirm not the problem but how they have qualified it and—more importantly—their confidence in its mitigation, whether that's the acceptance of the risk or prevention of it.

2. Cyberattacks have evolved from the equivalent of a single-celled organism into a complex life-form. Why is this important? It's important because cybersecurity has solved problem after problem, meaning that all too often we look for individual cells, to use the analogy, and in the modern world, this leaves us with lots of analysis (requiring expensive and slow human input) and often poor results. A house is built on solid foundations, yet in many ways, cybersecurity never had such foundations. Now is the time to step back and ask, "What foundations will allow your cybersecurity to work cohesively and effectively, both today and in the future?" Remember that technology is here to automate human processes, not the other way round!

3. Just how much overlap has evolved through the natural evolution? In the physical world, we complain every week that someone else is digging up the road for a different purpose, yet in cybersecurity, the same also occurs. Multiple technologies are repeating core processes (such as decoding network traffic) just so they can do their piece of the security analysis. In an ever more digital world, technical inefficiency is inexcusable.

   A big part of this is clearing out the deadwood. When something has worked for years, we are always reluctant to let it go, but as the effectiveness decreases, that's exactly what we should do. Challenge the security team on their effectiveness and clear out the deadwood.

4. At the heart of technology are zeros and ones (binary switches that make decisions). However, people use technology, and they are definitely not binary! Too much of cybersecurity is based on how

people should use technology, rather than how they do use it. It may be a hackneyed expression, but cybersecurity should enable, rather than inhibit, the business. If it's not doing that, then it's likely to be based on the principles of how technology should be used, rather than how it is being used.

5. One of the biggest challenges in cybersecurity today is validating what success actually is. Historically, some may have suggested this would be that nothing bad is happening, but the reality is that online, just as in the physical world, bad stuff happens every day. The question then is, "What is the goal of cybersecurity?" We can continue to respond to each instance, or we can aim for a more systemic solution. While new attacks take only minutes to produce, the underlying architecture they use typically remains constant. As such, rather than simply looking to stop the crime, we need to focus more on identifying the criminal methods being used, before they ever reach us. Compromised public systems and money flows all take time for the criminals to develop and should be considered part of the complex life-form we are looking to identify.

With the new legislation incoming, we have a rare chance to step back from being caught in the whirlwind of daily activities and evaluate just what 'good' looks like in cybersecurity. State-of-the-art cybersecurity is a dynamic requirement that requires regular review of what is possible, balanced against the real and relevant risks. Mixing modern capabilities with legacy ones is the equivalent of Usain Bolt running a three-legged race with you: he can go only as fast as you can, much in the way that your cybersecurity is limited by its legacy.

> In today's technology-driven world, the pace of change is relentless; as such, cybersecurity must continue to adapt to changing technology, new threats, and evolving business practices.

If I could give you one piece of guidance as we move into this era of 'state of the art', it would be to validate what success looks like in your business and what the state of the art should deliver to you in terms of protecting your business. Then test the reality, run what the industry calls 'red teaming' exercises (simulated attacks), including different functions of the business to see how well your state of the art stands up to scrutiny. Remember that the state of the art is dynamic, so this should be a regular exercise to ensure you remain current with the requirement and the best practices available. Lastly, discuss and compare with your industry peers to ensure you are getting a valid benchmark and drawing on the wisdom of crowds.