**Cyberspace**

Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.

Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.

Cyberspace allows users to share information, interact, swap ideas, play games, engage in discussions or social forums, conduct business and create intuitive media, among many other activities. The term cyberspace was initially introduced by William Gibson in his 1984 book, “Neuromancer.” Gibson criticized the term in later years, calling it “evocative and essentially meaningless.” Nevertheless, the term is still widely used to describe any facility or feature that is linked to the Internet.

According to many IT specialists and experts, including F. Randall Farmer and Chip Morningstar, cyberspace has gained popularity as a medium for social interaction, rather than its technical execution and implementation

**What Is Immersive Telepresence?**

Immersive telepresence is often known as virtual reality. This technology actually refers to the ability to create, remotely or in person, a [more realistic and powerful](http://www.telepresence24.com/2012/10/28/the-difference-between-video-conference-and-immersive-telepresence/) emotional and physical experience through digital equipment and software.

Avatars created online and interacting with other avatars is a form of [immersive telepresence](https://meetingsimagined.com/tips-trends/clever-carly-s-next-hot-topic-immersive-telepresence-aka-virtual-reality), but it also involves the depth of the immersion of the illusion into the reality of the audience. The stronger the immersion, the more the line between the digital representations and real participants is blurred. Telepresence simulates a real-life, 2-way encounter rather than the flat platform of traditional video conference with a video representation along with an audio feed. Simply stated, immersive telepresence mimics one or more participants being present in a remote location.

Many experts have asserted that the future of content consumption is immersive telepresence. Businesses will need to harness the power of this technology in order to remain competitive.

**What Are the Benefits of Immersive Telepresence?**

An obvious benefit of immersive telepresence is reducing travel costs and the associated travel-related stressors that accompany employees being brought to a location for meetings or training. This technology enables the users to experience the benefits of interacting as if on-location without the additional cost and hassle.

In addition to avoiding travel, immersive technology enables the users to experience the relationship-building, connection, and improved decision-making that once could only occur in real life face-to-face environments. Enabling co-workers or other team members to interact as if they were in the same room, despite being spread across the globe, creates endless opportunities for strengthening your business.

**Detection of attacks in cyberspace**

It is evident that organisations are struggling to prevent cyber attacks, despite significant investment. There is also growing realization that reliably detecting attacks is extremely difficult, with only one in five attacks being detected within a week after compromise (Verizon DBIR).

Effective detection is critical to establishing your cyber resilience. Responding to and recovering from an attack is largely contingent on the reliable, timely detection of a range of threats. We believe many organisations face the following detection challenges:

### **Excessive focus at the perimeter**

Modern attack techniques such as phishing are routinely successful at bypassing perimeter controls. If the attack isn’t detected at the perimeter, or by the user, most organisations struggle to prevent an attacker’s subsequent actions. It is therefore imperative that organisations turn their focus to post-exploitation detection; hunting for the steps an attacker within their environment must take to achieve their objectives.

### **Over reliance on technology**

While attention is shifting from the perimeter, to network level detection, to endpoint visibility, most organisations’ approaches remain over-reliant on automated technology. They expect the deployed technology to detect threats and serve them with alerts, using increasingly sophisticated analysis techniques, from event correlation and heuristics to machine learning.

Yet monitoring technology can be manipulated, and blindspots in coverage can be exploited. It is therefore not surprising that technology can be defeated or evaded by attackers skilled in breaking it.

### **Obsolete detection processes**

Many organisations have codified procedures for detecting attacks against their infrastructure, based on a short list of expected attack activity. However, the threat landscape and the actors within it evolve at such a rapid pace that many detection processes quickly become obsolete.

So, how can organisations get better at detecting advanced threats, especially considering the skills shortage that many are facing?

### **The opportunity to assess your detection capability**

Until recently the opportunities to assess detection capability were limited. Clearly organisations do not want to wait for an incident to learn of control failures. Red team exercises do provide a safer learning opportunity, yet they typically focus on a narrow set of activities, and fail to provide a broader appraisal of detection capability. And conventional assessments of security monitoring teams tend to focus on operational efficiency rather than effectiveness; doing things well, without necessarily doing the right things.

There are increasing opportunities to apply technological solutions to the challenges above, in different and more useful ways. One area is offensive security skills, a scarce yet integral part of building an effective detection capability.

In a post-exploitation situation, one needs to understand the stage an attacker is at, and crucially what their next move might be. This allows you as a defender not only to anticipate and intervene, while offering you the opportunity to go back and search in the right places for further information. Decisive action based on a clear understanding of the situation is more likely to result.

### **Specific detection tools**

Organizations have slowly woken up to this and are trying to bring the attacker mindset into their monitoring teams, either in the form of ‘purple teams’, where red team testers collaborate with the blue team, or through automated red teaming. At the heart of both approaches is the appetite to expose the monitoring team to more attacker tactics, techniques and procedures, including post-exploitation strategies. Maximising the learning opportunities here is key for development.

MWR’s experience and technical research has resulted in specific detection tools that have the potential to provide a much broader and more complete picture of the possible attack paths in your estate. In addition, your organisation’s ability to detect a range of attacker activities across the lifecycle of a modern attack is revealed, allowing you to properly equip your team with the capabilities and tools required.

Automated red-teaming forms part of our detection toolset. However, as with many tools, it has to be deployed in the right way to be really useful. It’s a technological solution to a human problem and it’s not possible to completely emulate a creative, unpredictable human adversary with technology. But, by supplementing your human red-teams with these automated tools, you can give yourself an even broader view of the weaknesses in your estate.

It’s no longer about simply understanding whether or not it’s possible to infiltrate your organisation. Rather, it’s about using every weapon in your armoury to understand as complete a picture as possible of all the ways an attacker might attempt to get in.

## **Install & Update Anti-virus & Other Cybersecurity Programs**

If you haven’t already installed anti-virus, anti-malware, and anti-spyware software on every device at your manufacturing facility, now is the time. Install, use, and regularly update these cybersecurity measures on every computer, tablet, and smartphone.

These mechanisms can help shield your company’s valuable data and information from malware, which is the catch-all term for malicious code. Written with the intent to steal or cause harm to information systems, malware contains viruses, spyware, and ransomware. Malicious code can not only steal your computer memory; it can also enable a cyber criminal to record your computer actions and access sensitive information.

To get the most out of your anti-malware programs, set the software to automatically check for updates at least once daily, or in real-time, if available. Adjust the settings to run a complete scan after daily updates.

An example of typical business anti-malware settings might include:

* Running anti-virus programs daily or nightly, such as at midnight
* Scheduling a virus scan to run about half an hour later (12:30 a.m.)
* Following up by running anti-spyware software a couple of hours later, such as at 2:30 a.m.
* Running a full system scan shortly afterward (3:00 a.m.)

This example is based on the assumption that a facility always has a running, high-speed Internet connection for all devices. The timing of your updates and scans may vary, but you need to perform them daily. Be sure to schedule them so that only one activity takes place at any given time.

For home-based employees or for employees’ personal devices, make sure they have copies or access to the same anti-virus and anti-spyware software, and require them to run regular updates per the previous example.

It is important that all employees understand why running anti-virus, anti-malware, and anti-spyware is vital to protecting company information and assets. Employees must also understand how early detection could potentially save the company from serious consequences associated with a cybersecurity incident or breach.

For redundant security, you may want to use two different anti-virus solutions from different vendors. Using anti-malware protection from two different providers can improve your chances of detecting a virus. Routers, firewalls, or Intrusion Detection and Prevention Systems (IDPS) usually have some anti-virus capabilities; but you don’t want to rely on them exclusively to protect your network.

Keep in mind that anti-virus solutions can only detect known viruses. If a new virus is developed and deployed, your anti-virus may not be able to detect it. It is important to keep your anti-virus solutions up to date in order to detect the latest viruses.

## **Maintain & Monitor Detection Logs**

Most malware protection and detection hardware and/or software is equipped with logging capability.

Check your user manual for instructions on how to:

* Use your logs to identify suspicious activity
* Maintain regular log records that are valuable in an investigation
* Back up logs regularly and save them for at least a year (although some types of information may need to be stored for longer)

For added peace of mind, consider hiring a cybersecurity professional to review your logs for any red-flag trends, such as an unusually large amount of time spent on a social media site or a high frequency of viruses consistently found on a single computer. This activity may indicate a serious information security problem that requires stronger protection.

Now that we’ve run through the right mechanisms for detecting a cyber threat, we’ll explore how to respond if you do detect an attack, in the fourth installment of our five-part series on “Cybersecurity for Manufacturers” from the [MEP National Network](http://bit.ly/mep-national-network).

For more advice on cybersecurity best practices for manufacturers, contact the cybersecurity experts at [your local MEP Center](http://bit.ly/mep-national-network).

**Intellectual property rights in cyberspace**

Intellectual Property Rights (IPR) and Cyber Laws cannot be disconnected and digital content requires protection. That is where we step in to assist You to secure your digital content through proper IPR registration.

‘Cyberspace’ is the non-physical domain over which the communication between computers takes place through computer networks. With the growth of technology every individual has a right of accessing cyberspace and sharing information, unless they are in conflict with cyber law.

In cyberspace, sometimes information is shared by a person, who is not the owner of the same, or the information which is private. Hence, privacy is violated, and one makes profit on another person’s creation. Such rights are protected under intellectual property rights. The types of IPR are:

Patent, Copyright, Trademarks, Trade Secrets, Industrial and Layout Designs, Geographical Indications etc. When these rights are violated in cyberspace there are several remedies available for the various types of violation

These types are mentioned below:

1.**Copyright Infringement:**

Copyright protection is given to the owner of any published artistic, literary, dramatic or scientific work over his work to exclude everyone else from using that work on his own name and thereby gain profit from it.

When these copyrighted articles are unauthorizedly used by anybody without the permission of the owner, this amounts to copyright infringement. When copies are made of commercial software which are distributed over the internet, and sold by a third person (other than owner), that amounts to be a copyright infringement. Copying website or blog content also amounts to a copyright violation.

**2.Software Piracy:**

It is also covered under sections of Indian Copyright Act. This is the illegal use of software by copying and distributing them among organizations, groups etc for business personal use.

This piracy can be of 3 types: Soft lifting, Software Counterfeiting, and Uploading-Downloading.

**3.Cyber squatting and Trademark Infringement:**

Trademarks are distinctive marks can be words, pictures, sound or shape which describes the nature and quality about a certain product to the user.

The lions roar of ‘Metro-Godwyn-Mayer’ or the word art of ‘Google’ are the trademarks for these respective companies, when these marks, whether registered or unregistered, are used are used by some other company on their product, that is called trademark infringement.

**Cyber squatting** is the process by which domain names are registered, sold,trafficked-in with the intention to make profit from the goodwill of someone else’s trademark in bad faith. Cyber squatting is a punishable offence.