:RESOLVER

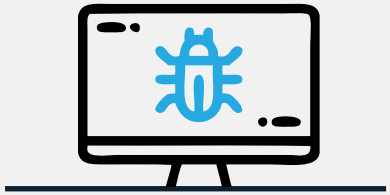
Guide to the Top 5 Corporate Security Threats of 2018

Is your organization equipped to weather these risks?

If 2017 was any indication, the future of the physical security industry and the nature of how organizations protect their people and their assets is quickly changing. Threats are increasingly ubiquitous and sophisticated, and organizations would be remiss not to take note. To kick off 2018, we've compiled a list of the top 5 corporate security threats organizations should be prepared for in the coming year:

1. New and Improved Cyber attacks

We think it's safe to say that 2017 had its fair share of cyber attacks that significantly impacted companies and consumers across the globe. From the Equifax hack that compromised the personal information of 143 million U.S. citizens to the infamous WannaCry attack perpetrated by North Korea that infected 300,000 computers, cyber attacks are systematically increasing in frequency, reach, and complexity.[1]



77% of companies

were hit by cyber attacks in 2017.

[1] Cranford, N. (2017). *The five worst cyber attacks of 2017*. [online] RCR Wireless News. Available at: https://www.rcrwireless.com/20171215/the-five-worst-cyber-attacks-of-20170tag27-tag99 [Accessed 19 Dec. 2017].

While the threat of cyber attacks is nothing new, the methods being employed to execute them continue to evolve. Once upon a time, insider threat and traditional email phishing were of primary concern to cybersecurity professionals. However, in today's landscape, threats are becoming progressively intricate. Cyber attacks may now manifest themselves in phishing powered by AI, a much more effective threat. In the near future, we'll likely see attacks so sophisticated that they'll render all of our current defences inept, such as attacks powered by quantum computing. Already we've seen AI used to modify malware to bypass the most advanced antivirus software defences.[2] Additionally in 2017 alone, 77% of companies were hit by cyber attacks.[3] This number is more than likely to rise in 2018.

Organizations must be prepared to both repel such threats, and recover from them quickly when their defences don't work. So, what is the best way to fight AI-powered cyber attacks? With more AI of course! By leveraging AI and machine learning, your organization will be more adequately prepared to detect and mitigate an AI-powered cyber attack. You can leverage AI and machine learning-based technology within your organization to bolster defences by automating and speeding up security operations. For example, such technology could be used to block malicious files and IPs and thus safeguard your organization against phishing attacks.[2] As determined by Cylance's polling, with 62% of security experts expecting AI to be weaponized and used for cyber attacks in 2018, there is certainly cause to be prepared.[4]

62% of security experts expect that AI will be weaponized and used for cyber attacks within the next 12 months, according to Cylance.

[2] DeNisco Rayome, A. (2017). *91% of cybersecurity pros fear hackers will use AI to attack their company*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/91-of-cybersecurity-pros-fear-hackers-will-use-ai-to-attack-their-company/ [Accessed 19 Dec. 2017].

[3] Samir, N. (2017). *77% of companies hit by cyber attacks in 2017 - Daily News Egypt*. [online] Daily News Egypt. Available at: https://dailynewsegypt.com/2017/12/17/77-companies-hit-cyber-attacks-2017/ [Accessed 19 Dec. 2017].

[4] Forrest, C. (2017). *62% of cybersecurity experts believe AI will be weaponized in next year*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/62-of-cybersecurity-experts-believe-ai-will-be-weaponized-in-next-year/ [Accessed 19 Dec. 2017].

2. Foreign Corporate Espionage

In the wake of allegations of Russian meddling in the recent U.S. election, intelligence agencies have been especially alert to signs of dubious foreign practices domestically. However, foreign powers are not just looking to infiltrate national elections. Over the course of the past year, foreign espionage has become of increasing concern to the corporate security world as well. According to the head of the FBI's counterintelligence agency, there has been a 53% rise in economic espionage cases in 2017 compared to 2016.[5] Unfortunately, this upward trend is likely to continue as foreign powers gain more technological literacy and are thus able to develop more sophisticated spying strategies. Moving into 2018, companies employing cutting edge techniques or developing innovative intellectual property will be most vulnerable to foreign espionage. With "the aim of economic espionage [being] to save a company the capital it would typically spend on research and development by just copying the processes of proven methods of production," it seems that some foreign powers feel this heinous tactic is a shortcut worth taking.[5]

Russia and China appear to pose the largest foreign espionage threat to the Western world. Given the recent bills banning the implementation of Kaspersky Labs' antivirus software for federal use in both the U.S. and the U.K., governments are evidently on high alert against foreign infiltration.[6] However, corporations and organizations should also be on their guard against such threats. Half of the 165 companies who participated in a survey issued by the FBI claimed to have been victims of economic espionage or intellectual property theft.[5] Further, 95% of the organizations who had been compromised claimed the attempts were from individuals associated with the Chinese government.[5]

53% increase in economic espionage

cases over the past year according to head of FBI's counterintelligence agency.

[5] Bruer, W. (2017). FBI sees sharp rise in economic espionage cases - *CNNPolitics*. [online] CNN. Available at: http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/index.html [Accessed 20 Dec. 2017].

[6] Hatmaker, T. (2017). *Trump signs bill banning Kaspersky Lab software from federal use*. [online] TechCrunch. Available at: https://techcrunch.com/2017/12/12/trump-signs-bill-banning-kaspersky-lab-software-from-federal-use/ [Accessed 19 Dec. 2017].

Surprisingly, foreign espionage is often conducted through seemingly innocuous means. In fact, an ICE agent recently accused Chinese drone company DJI Science and Technology of using its camera drone to spy on the United States.[7] The memo states "with moderate confidence that Chinese-based company DJI Science and Technology is providing U.S. critical infrastructure and law enforcement data to the Chinese government." Further, it "assesses with high confidence the company is selectively targeting government and privately-owned entities within these sectors to expand its ability to collect and exploit sensitive U.S. data."[7] While it's important to note that none of these allegations have been proven, in today's advanced technological landscape, such espionage tactics are at the very least plausible.

Even seemingly impenetrable organizations such as DuPont, Lockheed Martin, and Valspar have all been victims of foreign espionage in the past.[5] Frequently, organizations don't even realize they're being targeted. As such, it's imperative that corporate security teams are cautious and guard against any potential mishaps that may result in foreign infiltration by keeping employees informed of potential spy channels and vigilant in reporting suspected espionage attempts.

Half of the 165 private companies

surveyed by the FBI claimed to have been victims of economic espionage or intellectual property theft.

[7] Zhang, M. (2017). *US Says DJI Camera Drones Are Spying for China, DJI Calls Claim 'Insane'*. [online] PetaPixel. Available at: https://petapixel.com/2017/11/30/us-says-dji-camera-drones-spying-china-dji-says-claim-insane/ [Accessed 19 Dec. 2017].

3. Intellectual Property Theft

In the same vein as foreign espionage, within the current climate of rapid technological advancements, intellectual property theft—both foreign and local—is a serious concern for organizations today. The threat expands beyond economic repercussions and encompasses national safety and security as well. As such, the FBI has launched a nationwide campaign to warn industry leaders of this looming risk.[5] Even large companies such as Trimble, Siemens, and Moody's Analytics have recently been the victims of intellectual property theft.[8]

One of the main ways in which foreign entities succeed in stealing intellectual property is by bribing key current or former employees with large amounts of money. Andy Ubel, the chief intellectual property counsel at Valspar, recounts how "one of [the] key employees [at Valspar], a lab director, quit one day, and wouldn't tell [them] where he was going. [...] [They] only discovered later that he had downloaded a whole bunch of [their] data onto his own personal drive."[5] LinkedIn has also proven to be a valuable recruitment tool for foreign agents because of its granular search functionality that essentially makes any employee contactable by anyone.

While it may sound absurd, even the disposal of intellectual property must be properly executed to avoid "dumpster diving", as was the case when Chinese nationals were found digging in corn fields in Iowa in search of pest and drought resistant seeds developed by a U.S. company.[5] Cases of intellectual property theft have affected numerous industries, ranging from innovations in paint technology, synthetic fiber, seeds and grains, and military telecommunications.[5] Over the past year in the U.S. alone, hundreds of billions of dollars have been lost in the theft of trade secrets.[5]

Over the past year

in the U.S. alone,

hundreds of billions of dollars

have been lost in the theft of trade secrets.

[8] Perez, E. (2017). *US charges 3 Chinese nationals with hacking*. [online] CNN. Available at: http://www.cnn.com/2017/11/27/politics/china-hacking-case/index.html [Accessed 20 Dec. 2017].

However, organizations need not only be concerned by the risk of foreign intellectual property theft. As is evident by the most recent Uber scandal, national competitors may be just as much—if not more— of a threat than foreign ones. There is an ongoing court battle raging between Uber and Google over the alleged intellectual property theft of Google subsidiary Waymo's self-driving technology. The supposed theft took place when a key Waymo employee quit to work at Uber and took the technology in question with him when he left. Sound familiar? The threats are the same and as such, the safeguards that need to be implemented to mitigate such threats are the same.

Obviously within the Western world, the government plays a large part in securing intellectual property rights, especially when disputes arise between two organizations within the same country. Unfortunately, however, according to the U.S. Chamber of Commerce's annual IP index, after years as number one, the U.S. is now number 10 in patent protection.[9] This decreased emphasis on patent protection is problematic given the continuous trend towards innovation in technology. As such, the role corporate security teams play in ensuring their organizations' patents stay protected is increasingly critical. In order to mitigate intellectual property theft, it's imperative that organization drive proper internal awareness of potential threats and train employees on how to be vigilant and safeguard against any such threats. For example, conducting routine training on potential theft scenarios and continuously disseminating up-to-date information on at-risk channels will prove invaluable in defending against intellectual property theft caused by accidental insider threat.

After years as number one, the U.S. is now number 10 in patent protection according to the U.S. Chamber of Commerce's annual IP index.

[9] Manning, R. (2017). *Finally, a big international win for intellectual property rights.* [online] TheHill. Available at: http://thehill.com/opinion/technology/362197-finally-a-big-itc-win-for-intellectual-property-rights [Accessed 20 Dec. 2017].

4. Natural Disasters

2017 can easily be dubbed the year of natural disasters. According to 41/59 recent studies analyzed by the Energy and Climate Intelligence Unit, climate change has made extreme weather events longer and more intense.[10] The U.S. experienced 15 natural disasters costing at least $15 billion in damage in 2017 alone.[10] The author of the report, Richard Black, states that the findings show "specific events are made more likely or more damaging by climate change".[11] As such, the need to be ready for a potentially catastrophic natural disaster has never been greater.

While some establishments have been preparing for the worst case scenario since their inception—did you know that The Getty Museum has a million-gallon water tank and an air filtration system that keeps out smoke to protect itself against ever-threatening wildfires?—most others are only recently coming to terms with the idea that natural disasters are a serious cause for concern.[12]

Every $1 spent on disaster preparedness can prevent $7 worth of disaster-related economic losses, according to a study by Boston University.

[10] Nace, T. (2017). *Forbes Welcome*. [online] Forbes.com. Available at: https://www.forbes.com/sites/trevornace/2017/12/15/how-technology-is-advancing-emergency-response-and-survival-during-natural-disasters/#769c2b389cc8 [Accessed 20 Dec. 2017].

[11] Gabbatiss, J. (2017). *Natural disasters increasingly linked to climate change, new report warns*. [online] The Independent. Available at: http://www.independent.co.uk/environment/climate-change-natural-disasters-link-increase-global-warming-report-warning-a8103556.html [Accessed 19 Dec. 2017].

[12] Zhang, S. (2017). *What It's Like to Evacuate a Museum in a Natural Disaster*. [online] The Atlantic. Available at: https://www.theatlantic.com/science/archive/2017/12/museum-evacuation/547514/ [Accessed 20 Dec. 2017].

However, there is a silver lining to this unavoidable threat. While future natural disasters may continue to increase in frequency and intensity, we've also developed more sophisticated tools that can be leveraged to stay informed about potentially harmful or dangerous weather conditions. For example, internet of things sensors can be used to detect how far and how fast wildfires are spreading or to monitor water levels in the case of tsunamis or hurricanes and send alerts at the first sign of flooding.[13] Further, sensors can be used to detect the presence of harmful gases or chemicals emanating from a storage tank, factory, or plant. This type of information is critical in judging when to evacuate an area or how to guide residents to the safest exit routes when an emergency strikes.[13] Additionally, a tool to send mass notifications to employees or facility visitors is especially important when it becomes necessary to communicate an emergency or enforce emergency protocol. Implementing routine drills on more common disaster scenarios can also be beneficial in ensuring emergency teams and employees are well-versed on what to do in a given situation. However, the most important thing is to be prepared when disaster does strike. As such, organizations should be equipped with a comprehensive natural disaster preparedness plan. In fact, according to a study by Boston University, for every $1 spent on disaster preparedness, $7 worth of disaster-related economic losses can be prevented.[14]

In 2017, the U.S. had

15 natural disasters

that resulted in over

$15bn in damages.

[13] Tremaine, K. and Tuberson, K. (2017). *How the Internet of Things Can Prepare Cities for Natural Disasters*. [online] Harvard Business Review. Available at: https://hbr.org/2017/12/how-the-internet-of-things-can-prepare-cities-for-natural-disasters [Accessed 20 Dec. 2017].

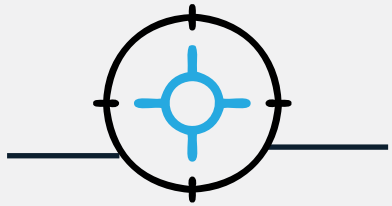
[14] Zeliff, T. (2017). *Can Your Organization Survive a Natural Disaster?; Digiscribe*. [online] Digiscribe. Available at: http://www.digiscribe.info/blog/can-your-organization-survive-natural-disaster/ [Accessed 20 Dec. 2017].

5. Lone wolf and homegrown terrorism

Lone wolf terrorism is typically defined as an individual "acting alone or with one or two others, without specific instructions, with a political motivation but no formal ties to an organization."[15] Usually the "perpetrator is a long-term resident in the target country and has completed the process of radicalization there".[16]

In today's divided world, there has been a spike in homegrown and lone wolf terrorism not just in the U.S., but across Europe as well. According to a recent study, 73% of attacks in Europe and North America were carried out by homegrown terrorists over the past three years.[16] These amateur, minimally-involved threats are often the hardest to detect and almost impossible to foil. Thus, security teams must increasingly be on the lookout for potential threats within their organizations—whether amid their employees or amid their employees' networks.

Recent homegrown terrorist attacks—notably the 2017 Las Vegas attack, the 2017 Manchester attack, the 2016 Orlando attack, and the 2016 Nice attack, resulted in over 200 fatalities and hundreds more injuries. Of the 100 terror attacks in the U.S. since 9/11, 87 have been homegrown terrorist attacks.[16] However, extremist violence does not just come in the form of radicalized foreign Islamists. Of the three terrorist attacks that occurred in New York City in 2017, each terrorist was a legal immigrant to the U.S. and had been radicalized on U.S. soil. Further, the lone wolf shooter during the October 1, 2017 Las Vegas massacre was similarly homegrown—and wasn't not even from an immigrant background. In fact, more Americans have been killed by native white U.S. men in 2017 than by any radical Islamists.[17] Furthermore according to New America, between 2001 and 2015, more Americans were killed by homegrown right-wing extremists than by Islamist terrorists.[17] More disturbingly, none of these terrorists offered many clues to their intentions. As such, it's important to stay vigilant and open-minded about who could be a potential assailant.



73% of attacks in Europe and North America

were carried out by home-grown terrorists over the past three years according to a recent study.

[15] Strohm, C. (2017). *Lone-Wolf Terrorism*. [online] Bloomberg Quint. Available at: https://www.bloombergquint.com/quicktakes/2017/12/11/lone-wolf-terrorism [Accessed 20 Dec. 2017].

[16] Fu, Y. (2017). *Tackling the Wave of Homegrown Terrorism*. [online] IPP Review. Available at: https://ippreview.com/index.php/Blog/single/id/612.html [Accessed 20 Dec. 2017].

[17] Williams, J. (2017). *White American men are a bigger domestic terrorist threat than Muslim foreigners*. [online] Vox. Available at: https://www.vox.com/world/2017/10/2/16396612/las-vegas-mass-shooting-terrorism-islam [Accessed 20 Dec. 2017].

Although lone wolf terrorism is difficult to prevent, insight into an individual's mental health can provide some telling clues. One study found a lone wolf is 13.5 times more likely to have a mental illness than a terrorist acting within an organization.[15] It's thus critical that corporate security teams work closely with their respective human resources departments to stay informed of any potential red flags. Employers should offer free psychological assessments and relevant mental health resources for employees. Human resources departments should additionally conduct regular check-ins to ensure employees are reasonably content and don't appear to be at-risk of violence or the victims of violence at home. Employees should further be encouraged to report any concerns or complaints of suspicious behaviour—whether observed within the organization or externally—whereby security teams can conduct proper follow up and, if necessary, investigations. Finally, in terms of response protocol, corporate security teams should always be prepared with on-the-ground security personnel in the event that an attack does take place.

87/100 terror attacks

in the U.S. since 9/11 have been

homegrown terrorist attacks.

Protect Your Organization with Resolver

At Resolver, we understand how important it is to ensure your employees, customers, supply chain, brand, and shareholders are safe—that's why over 1000 of the world's largest companies use us to protect what matters.

Resolver's approach to corporate security is simple: we build software that enables organizations to better plan and prepare to limit the likeliness of threats from occurring, and more effectively respond and recover to minimize impact when they do. Our platform combines risk and site assessment, enterprise security risk management (ESRM), incident management and reporting, investigations and case management, command center, workplace threat assessment, brand protection, and loss prevention into one tool to meet all of your corporate security needs.

Get the insight, information, and tools that you need to optimize your corporate security efforts with Resolver.

Plan. Prepare. Respond. Recover.

Works Cited

Belot, H. (2017). *Turnbull to ban foreign donations, force agents to declare international links*. [online] ABC News. Available at: http://www.abc.net.au/news/2017-12-05/turnbull-announces-foreign-interference-laws/9227514 [Accessed 19 Dec. 2017].

Bond, D. (2017). *UK spying fears spark Russian software ban*. [online] Ft.com. Available at: https://www.ft.com/content/d323c458-d6a4-11e7-8c9a-d9c0a5c8d5c9 [Accessed 19 Dec. 2017].

Bruer, W. (2017). *FBI sees sharp rise in economic espionage cases - CNNPolitics*. [online] CNN. Available at: http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/index.html [Accessed 20 Dec. 2017].

Cranford, N. (2017). *The five worst cyber attacks of 2017. [online] RCR Wireless News*. Available at: https://www.rcrwireless.com/20171215/the-five-worst-cyber-attacks-of-20170tag27-tag99 [Accessed 19 Dec. 2017].

DeNisco Rayome, A. (2017). *91% of cybersecurity pros fear hackers will use AI to attack their company*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/91-of-cybersecurity-pros-fear-hackers-will-use-ai-to-attack-their-company/ [Accessed 19 Dec. 2017].

Forrest, C. (2017). *62% of cybersecurity experts believe AI will be weaponized in next year*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/62-of-cybersecurity-experts-believe-ai-will-be-weaponized-in-next-year/ [Accessed 19 Dec. 2017].

Fu, Y. (2017). *Tackling the Wave of Homegrown Terrorism*. [online] IPP Review. Available at: https://ippreview.com/index.php/Blog/single/id/612.html [Accessed 20 Dec. 2017].

Gabbatiss, J. (2017). *Natural disasters increasingly linked to climate change, new report warns*. [online] The Independent. Available at: http://www.independent.co.uk/environment/climate-change-natural-disasters-link-increase-global-warming-report-warning-a8103556.html [Accessed 19 Dec. 2017].

Hatmaker, T. (2017). *Trump signs bill banning Kaspersky Lab software from federal use*. [online] TechCrunch. Available at: https://techcrunch.com/2017/12/12/trump-signs-bill-banning-kaspersky-lab-software-from-federal-use/ [Accessed 19 Dec. 2017].

Manning, R. (2017). *Finally, a big international win for intellectual property rights*. [online] TheHill. Available at: http://thehill.com/opinion/technology/362197-finally-a-big-itc-win-for-intellectual-property-rights [Accessed 20 Dec. 2017].

Nace, T. (2017). *Forbes Welcome*. [online] Forbes.com. Available at: https://www.forbes.com/sites/trevornace/2017/12/15/how-technology-is-advancing-emergency-response-and-survival-during-natural-disasters/#769c2b389cc8 [Accessed 20 Dec. 2017].

Perez, E. (2017). *US charges 3 Chinese nationals with hacking*. [online] CNN. Available at: http://www.cnn.com/2017/11/27/politics/china-hacking-case/index.html [Accessed 20 Dec. 2017].

Samir, N. (2017). *77% of companies hit by cyber attacks in 2017 - Daily News Egypt*. [online] Daily News Egypt. Available at: https://dailynewsegypt.com/2017/12/17/77-companies-hit-cyber-attacks-2017/ [Accessed 19 Dec. 2017].

Strohm, C. (2017). *Lone-Wolf Terrorism. [online] Bloomberg Quint*. Available at: https://www.bloombergquint.com/quicktakes/2017/12/11/lone-wolf-terrorism [Accessed 20 Dec. 2017].

Tate, C. (2017). *Latest NYC terror attack shows how tough it is to stop a lone wolf*. [online] USA TODAY. Available at: https://www.usatoday.com/story/news/nation-now/2017/12/11/lone-wolf-terror-attacks/942750001/ [Accessed 20 Dec. 2017].

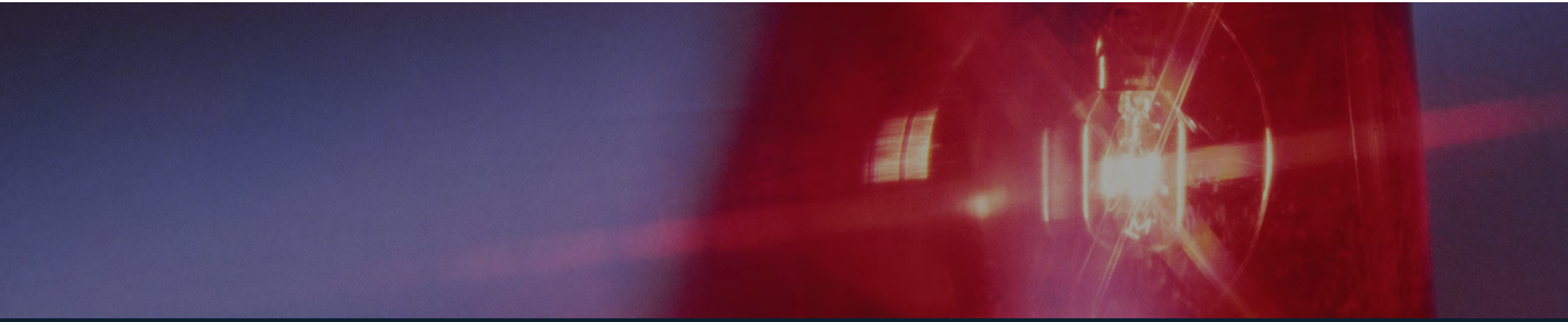
Tremaine, K. and Tuberson, K. (2017). *How the Internet of Things Can Prepare Cities for Natural Disasters*. [online] Harvard Business Review. Available at: https://hbr.org/2017/12/how-the-internet-of-things-can-prepare-cities-for-natural-disasters [Accessed 20 Dec. 2017].

Williams, J. (2017). *White American men are a bigger domestic terrorist threat than Muslim foreigners*. [online] Vox. Available at: https://www.vox.com/world/2017/10/2/16396612/las-vegas-mass-shooting-terrorism-islam [Accessed 20 Dec. 2017].

Zeliff, T. (2017). *Can Your Organization Survive a Natural Disaster?; Digiscribe*. [online] Digiscribe. Available at: http://www.digiscribe.info/blog/can-your-organization-survive-natural-disaster/ [Accessed 20 Dec. 2017].

Zhang, M. (2017). *US Says DJI Camera Drones Are Spying for China, DJI Calls Claim 'Insane'*. [online] PetaPixel. Available at: https://petapixel.com/2017/11/30/us-says-dji-camera-drones-spying-china-dji-says-claim-insane/ [Accessed 19 Dec. 2017].

Zhang, S. (2017). *What It's Like to Evacuate a Museum in a Natural Disaster*. [online] The Atlantic. Available at: https://www.theatlantic.com/science/archive/2017/12/museum-evacuation/547514/ [Accessed 20 Dec. 2017].



Want to learn more? Let's talk.

resolver.com | info@resolver.com | 1-888-891-5500