SMART RAIL WORLD

APRIL 2017
ISSUE #23

PROTECTING RAIL AND METRO FROM CYBER SECURITY THREATS

WALLS DON'T WORK! Why a change is needed in rail industry thinking about cybersecurity

HOW hackers breached San Francisco's transit system and demanded a $73,000 ransom.

WATERFALL SECURITY'S Lior Frenkel on cyber threats to the rail industry.

Digital Guide Sponsors:

RazorSecure

WATERFALL
Stronger Than Firewalls

Contents

2 Editor's Welcome.

3 Waterfall Security's Lior Frenkel on cyber threats to the rail industry.

6 Walls don't work! Why a change is needed in rail industry thinking about cybersecurity.

8 Expert Insights - Jonathan Risto, Community Instructor, SANS.

11 How hackers breached San Francisco's transit system and demanded a $73,000 ransom.

12 More Than 75% of Crypto Ransomware in 2016 Came From the Russian-Speaking Cybercriminal Underground.

14 Terror train wreck threat from new rail signal system – security specialist.

SMARTRAIL WORLD

Dear colleague,

Many thanks for downloading '**Protecting Rail and Metro from Cyber Security Threats**' the 23rd digital guide from the team at SmartRail World.

"One morning, you get a message flashing up on a screen in a control room demanding $200,000 or the train will be derailed. And then you pay. This is how serious the threat is. And I know of at least one incident similar to this."

What connects the San Francisco Municipal Transportation Agency with the Democratic National Committee in the USA, London's Barts hospital, the Bundestag in Germany, the Japanese Ministry of Defense, Facebook, Twitter, Netflix and thousands of other businesses both large and small?

They were all victims of cyber-crime in 2016.

The past year has seen a significant rise in cyber security breaches, and rail and metro operators are increasingly being targeted. They are vulnerable to losing control of three key areas; the operational aspect of the trains themselves, fare collection systems and the increasingly large amount of data being harvested be it of a technical, financial or personal nature. And the rapidly increasing digitisation of all these aspects is accelerating the opportunity for cyber criminals. If access to mission critical and safety systems is compromised, the results could be fatail.

Network Rail, the owner and operator of most of the UK rail infrastructure have acknowledged the threat stating; "We know that the risk [of a cyber-attack] will increase as we continue to roll out digital technology across the network." In San Francisco we saw a ransomware threat whereby criminals gain entry to your system, encrypt the data and then demand a ransom to decrypt it. The battle to keep ahead of the cyber-criminals will be a part of all our futures. Ransomware attacks have been the most common type of cyber criminal activity in the past year.

This is an area of the industry that is crucial for the industry, so we decided to publish our first guide dedicated to the subject to help support rail and metro operators from around the world to ensure they can keep pace with the cyber criminals.

This guide wouldn't have been possible without the expertise and support from our partners Waterfall Security whose mission is to revolutionize the way industries protect their physical assets and processes from cyberattack and RazorSecure who was founded in 2014 to address a key gap in the cyber security market.

We'd also like to thank the industry experts at Alcatel-Lucent, SANS INSTITUTE and ELERTS for their support.

This is an area that we are keen to focus further on, so if you would like to contribute to future features and publications, please e-mail me Luke.Upton@GlobalTransportForum.com

Many thanks to all the contributors for sharing their time and helping make this guide happen.

Regards and thanks,

Luke Upton
Editor
SmartRail World
www.smartrailworld.com

@SmartRail World | @SmartRail World News | SmartRail World | SmartRail World | futureurbanmobility

Waterfall Security's Lior Frenkel on cyber threats to the rail industry.

A firewall is a device that has been the first line of defence in network security for over 25 years, but is it the right cybersecurity solution for a rails system? A firewall is essentially a router with a set of rules with the security provided by the software. Every software in the world has bugs and vulnerabilities, and any line of code can be exploited. The security that is provided is considerable- but you can easily manipulate and reconfigure it, making it possible to acquire access to the rails signalling network.

As public transport is undergoing digital transformation, and our industry becomes more reliant upon it, the attack surface for potential damage is massively increased. Clearly, traditional firewalls are not secure enough to keep pace with the progressively sophisticated attacks from hackers and cyber criminals.

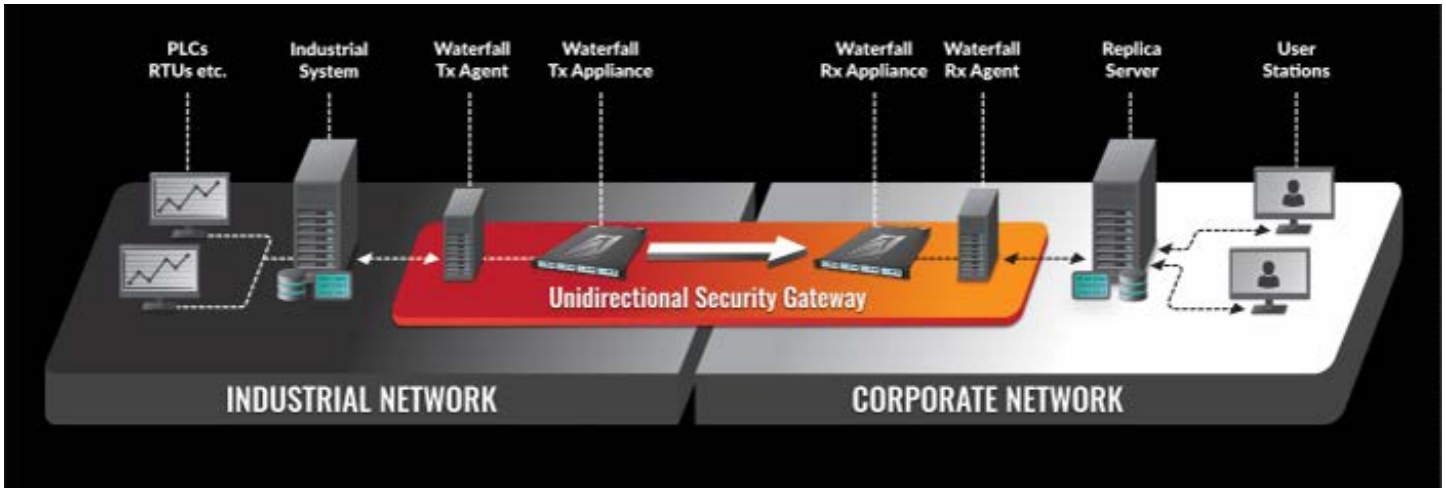
Fortunately, since 2007 **Waterfall Security** has pioneered a different approach to industrial cybersecurity technology. An Israeli company with customers worldwide, Waterfall keeps industrial networks secure with innovative "unidirectional security gateway" technology that provides a stronger alternative to firewalls. With this guide focussed on helping rail and metro operators develop the tools needed to combat cyber threats, our Editor Luke Upton recently spent some time with Waterfall Security's CEO and Co-founder Lior Frenkel and discussed why they have taken this different approach, what some of the specific threats are and why rail companies should not depend on firewalls or other IT-based cybersecurity to protect their control and SCADA systems.

Waterfall Security began its work a decade ago servicing the power industry and quickly branched out into other sectors, including public transportation where they now work with metros and railways around the world (who for security reasons must remain anonymous). Although there have been a number of recent cybersecurity breaches, most notably on the San Francisco Metro, most passengers are unaware of the complex systems that ensure they have a successful journey. To maintain the safety of passengers and the reliability of operations, cybersecurity has become a paramount concern for rail and metro transportation.

"Yes, there is always a threat from disgruntled former employees or from individuals in a group of particular countries but today, ransomware is where the principal threat exists."

"Despite hundreds of millions of people utilizing public transport every day, most countries don't have specific regulations relating to cyber security, with the exception of the Department for Transport in the UK. But rail and metro operators know that today's threats are extremely dangerous, as any cyberattack can lead to crash or derailment. Lior explains, "The biggest risk to industrial networks occurs when there is a connection to an external network. In many ways, connecting rail systems to the internet is quite reckless, but delivers so many efficiencies that it's hard to see a day when public transport won't be connected. What is most concerning is when the mission-critical control systems are connected to the same networks used by the passengers or the business networks. Here you open up the control system to the bad guys, who needn't even be on-board the train to find a way into the control system."

Waterfall Security has developed the 'unidirectional security gateway' technology to prevent remote cyberattacks from entering a control network, while providing a critical need for visibility and access to real-time data by headquarters or remote personnel without opening up the network to any Internet connections. The Unidirectional Security Gateway is physically incapable of propagating any virus, DOS attack, ransomware, malware, human error or any information at all into the control network.



Waterfall Security's Lior Frenkel on cyber threats to the rail industry. *[cont]*

Information can only flow out of the control network to a business network – only in that one direction. "Just like the one-way flow of water in a waterfall, hence the name," adds Frenkel.

This solution is considered as cybersecurity best practices by many regulatory and governmental agencies, including the Department for Transport in the UK. In addition to its use in railways and metros, Waterfall's Unidirectional Security Gateway can be found deployed in utilities, nuclear plants, on/off-shore platforms, refineries, manufacturing plants, and other industries.

With the time so far focussing on the solutions, Luke was keen to learn more from Lior, a widely respected expert in this field, with over 20 years' experience about some of the specific threats, and asked, "Where do these threats originate from?"

"These days in rail and metro, the threat comes from criminals using ransomware to extort money from operators. One morning, you get a message flashed up on a screen in a control room demanding $200,000 or the train will be derailed. And then you pay. This is how serious the threat is. And I know of at least one incident similar to this. Yes, there is always a threat from disgruntled former employees or from individuals in a group of particular countries but today, ransomware is where the principal threat exists."

"Another danger that I want to highlight is that the growth of the Internet of Things (IoT) has led to a proliferation of connected devices aboard a train, some even as basic as a "smart coffee pot" in the buffet car. These are often very cheap systems, with little or no security. In these cases, where the signalling network can be accessed through the passenger network, the "smart coffee pot" network access becomes an entry point for hackers. As CEO of Waterfall, this threat means more business, but as a private citizen I find it very concerning."

Business networks are under constant attack and similarly, the control and signalling networks that operate our trains and metros are no different. For Waterfall, firewalls are "just a bump when you need a wall" and when it comes to intrusion detection systems "it's too late to stop an attack." How transport professionals deal with this threat is one of the major challenges of modern business. As Lior says, "Stay ahead of the bad guys" by focussing on the prevention of attacks, eliminating remote online attacks from entering your controls - something which Waterfalls' evolutionary alternative to firewalls provides.

Waterfall Security Solutions is a privately-owned company with its headquarters based in Israel, and sales and support operations in North America, Europe and Asia.

WATERFALL Stronger Than Firewalls

For more information visit **www.waterfall-security.com,** email: **info@waterfall-security.com** or call +1 703 840 5452.

They can also be found on Stand 17 at the **SafeRail Congress,** Washington D.C. April 11-12.

"Despite hundreds of millions of people utilizing public transport every day, most countries don't have specific regulations relating to cyber security, with the exception of the Department for Transport in the UK."

Walls don't work! Why a change is needed in rail industry thinking about cybersecurity.

National governments, all over the world, are now acutely aware of the threat that cyber-attacks pose to their country's infrastructures and are taking steps to protect their citizens. Many have already introduced new standards and guidelines for both rolling stock and infrastructure; the US has issued an Executive Order for the Enhancement of National Cybersecurity and, in the UK, a new mandatory framework will come into force in May 2018.

Ahead of the introduction of these regulations, changes are already being seen with more stringent cyber-requirements being included in tenders for new trains. Train operators understand that they must comply with the laws but they also see the huge threat to brand value that would result from a successful attack. The broadening of on-board services beyond passenger Wi-Fi to more complex systems involving Infotainment, CCTV and real-time Information is also increasing the need for enhanced security solutions to deal with the myriad threats. With security protocols already in place within other aspects of organisations, adequately safeguarding the vehicle fleet itself is a timely demand.

The new cyber-guidelines coming into play have a common theme; namely, that 'walls don't work'. Throughout the industry, there is a tacit admission that the protection of critical assets will need more than just using traditional methods such as firewalls, Virtual Private Networks (VPNs) and authentication. A single line of defence is often not enough because if one back-door is found, an intruder can exploit it to enter the whole system. It's also widely accepted that cybersecurity is a process, rather than a binary on/off state; for rail operators, becoming secure is an ongoing development of testing, evaluating and deploying new defences.

This layered approach, known as 'Defence in Depth', provides active protection and is recognised as the best way to secure the core of the systems, especially when outer layers (such as firewalls) have been breached. In this framework, a variety of methods and tools are used together in synchronisation to form a more powerful protective web around a network. Active protection that will 'Monitor, Detect, Report and Protect' (MDRP) is agreed to be the gold standard defence when supported by regular auditing and a security operations centre (SOC).

The transport industry is increasingly viewed as a viable target for cybercriminals; traction systems, train control systems, passenger information systems and station infrastructure are all potentially at risk. Cyber-criminals may decide to attack ticket machines, passenger information displays and passenger Wi-Fi systems. However, providers of these systems face a dilemma; how to comply with the new standards without replacing or adding more hardware? Trains can't be updated like data centres and have a unique set of requirements that can't be met with traditional solutions alone.

RazorSecure, the Transport Cybersecurity Specialist, has developed a purely software-based, MDRP solution called RazorSecure Delta. RazorSecure Delta protects the core when the wall has been breached. The software uses sophisticated machine-learning to actively protect the systems on trains and many other forms of transport, whether they are connected or not. RazorSecure work with existing system suppliers, such as Icomera, to implement active security at a fraction of the cost of hardware-based versions.

Walls don't work! Why a change is needed in rail industry thinking about cybersecurity. *[cont]*

To address the need for regular auditing, RazorSecure will be launching RazorSecure Edge, a remote penetration testing unit which removes the need for a pen test consultant to visit the train or the site.

Robert Brown, RazorSecure Executive Chairman, commented that "from working on the first passenger Wi-Fi systems a decade ago, the focus has moved from passengers to other applications that can exploit the use of the bandwidth. I predict the next challenge is how do we protect our systems from the new and unfolding threat of aggressive cyber-attacks from some very unsavoury characters."

Icomera has installed systems on thousands of trains around the globe and their networks carry more than 37 TB per day, primarily from more than half a million passengers using on-board Wi-Fi – naturally, cybersecurity is an extremely important consideration and Icomera systems already have a high degree of protection built into them. However, they too see the merit in the Defence in Depth approach.

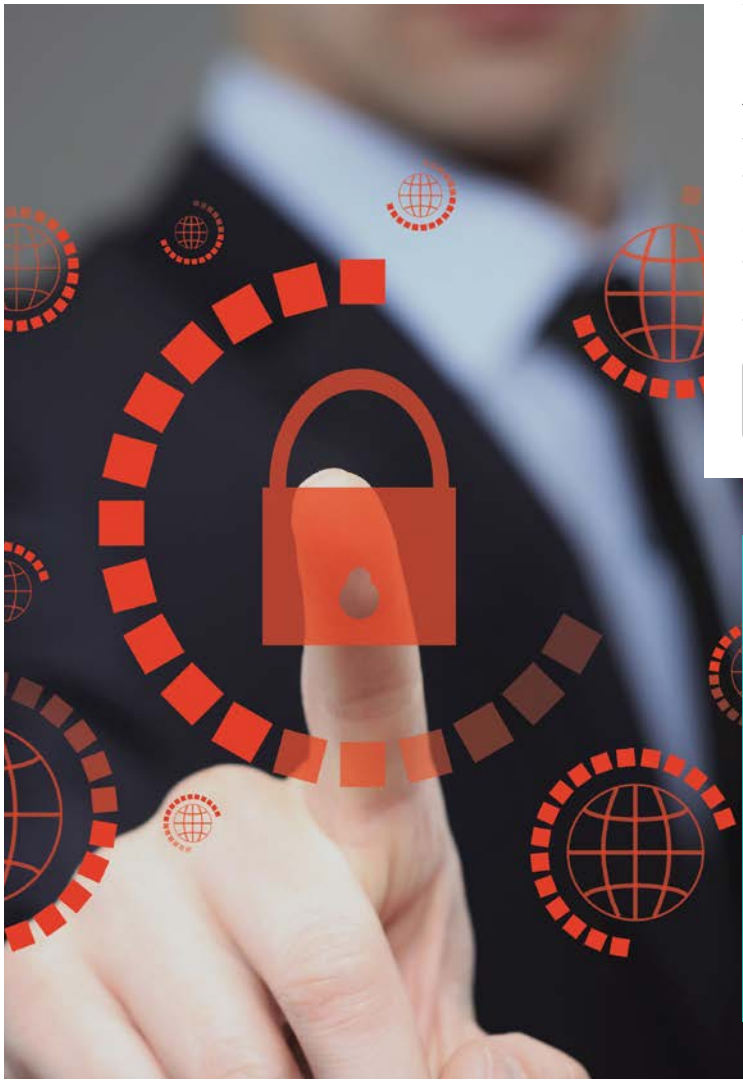
As Daniel Jaeggi, Head of Business Development at **Icomera**, explains, "The world is changing quite rapidly: cybersecurity threats are becoming extremely sophisticated and more and more systems are being connected to our on-board networks, increasing the attack footprint. At the same time, customers are putting in place more robust cybersecurity processes, mostly in response to a greater awareness of the risks and financial impact from cyber-attacks. So, we're seeing strong demand for higher levels of assurance and monitoring, and we're working closely with customers and providers such as RazorSecure to meet this need."

At the heart of the Defence in Depth approach is the assumption that any system, no matter how well engineered or secured, may be vulnerable to a cyber-attack. Better engineering can only take you so far; active monitoring and second-line protection is needed to enhance network security. This can be a hard concept to fully grasp. However, as Daniel Jaeggi points out, this assumption of fallibility is common in many other areas where security and safety are paramount: "When you board a flight, your pilot can be the best in the world, but all the safety systems and processes are designed around the idea that he or she will make mistakes or systems fail that shouldn't. Things go wrong, that shouldn't be a problem in itself, it's how you deal with them and what backup you have. That's what keeps you safe!"

This shift in thinking is required to bring on-board networks up to the next level of security, and both RazorSecure and Icomera are already jointly offering rail operators enhanced, software-based protection which integrates seamlessly with existing on-board hardware. Through deploying additional protective tools and actively monitoring a system, businesses will benefit from increased Defence in Depth and become better equipped to detect and respond to cyber-attacks in the future.

RazorSecure

For more information visit **www.razorsecure.com** or email: **sales@razorsecure.com**



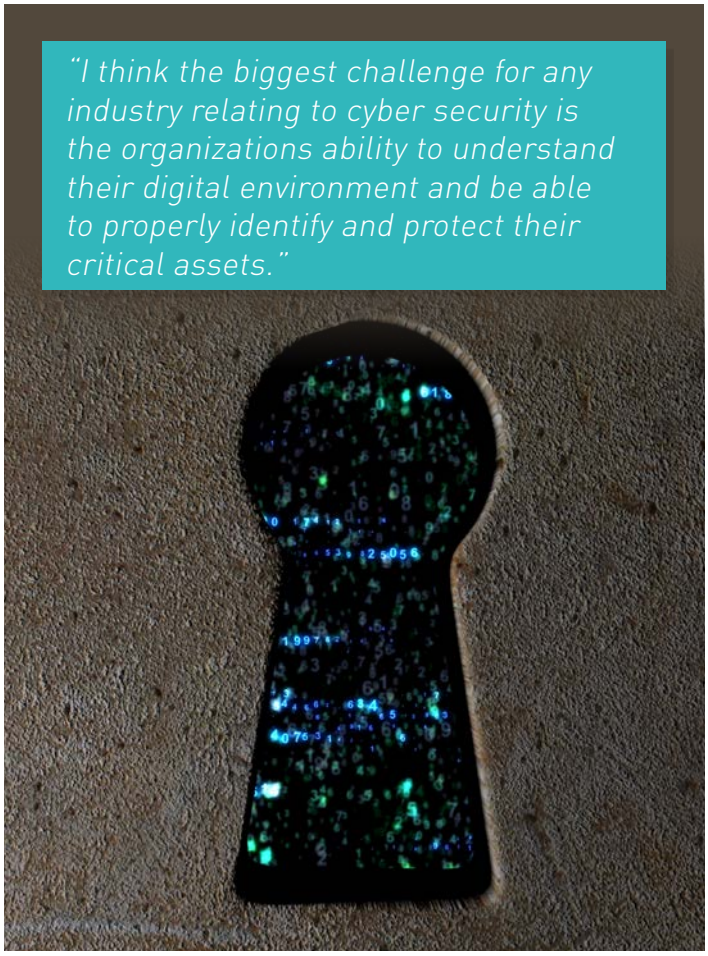
The new cyber-guidelines coming into play have a common theme; namely, that 'walls don't work'. Throughout the industry, there is a tacit admission that the protection of critical assets will need more than just using traditional methods such as firewalls, Virtual Private Networks (VPNs) and authentication. A single line of defence is often not enough because if one back-door is found, an intruder can exploit it to enter the whole system.

Expert Insights - Jonathan Risto, Community Instructor, SANS.

Today we are speaking to Jonathan Risto, a mentor and community instructor at SANS, global leader in cyber security. He teaches in the areas of intrusion detection, incident handling, penetration testing and security management. When not teaching for SANS, he works for the federal government performing cyber security research. He has just completed his Masters of Information Security Management degree from SANS Technology Institute and has published numerous papers in cyber security. He currently holds a variety of industry certifications that include 11 GIAC certifications and is a licensed Professional Engineer.

Luke Upton (LU): Thanks for your time today, we are looking forward to your training session at the upcoming SafeRail Congress, could you give us a sneak preview of some of the key areas you'll be focussing upon?

Jonathan Risto (JR): Thank you for providing me with the opportunity today. The course that SANS is offering at SafeRail is Security 440, Critical Security Controls: Planning, Implementing, and Auditing. This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls, are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the controls are effectively implemented.One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That ensures the defenses very real, and it makes you a better security professional.



LU: You have over 17 years of experience in the technology space, what has brought you into working with digital security?

JR: I have always been interested in computers, even while growing up. That interest carried right though to my university studies, which was in Computer Engineering. With degree in hand, I went to work at a large telecommunications company performing Local Area Network (LAN) and Wide Area Network (WAN) network design, configuration and implementation. At the time, this also tended the include items such as firewalls and the basic controls we had for our networks. This was at the height of the tech boom, and everything was exploding online. And so were the security concerns. It was fun, it was challenging, and I like a challenge. As time progressed, I focused solely in security. Architecture and design, configuration and implementation, it didn't matter. Then at one of my jobs, I was the security operations prime, and I went and took a course from the SANS Institute. WOW. From the first few minutes in that class until the end of day 6, it was a constant overflow of information that was completely relevant to and feasible to use when returning back to work. Within a year, I started working with SANS, mentoring and then teaching the classes, and I have loved every minute of it! I have loved every minute of it.

LU: In your professional opinion, what is the single biggest threat to the rail and metro industry from digital attacks?

JR: I think the biggest challenge for any industry relating to cyber security is the organizations ability to understand their digital environment, be able to properly identify and protect their critical assets. We cover this in the SEC440 course, and provide a prioritized listing of the security measures that will help anyone secure their network. There are so many facets to security, we need to be good at all of them. It takes one small mistake, and then the bad guys can gain access to our network. But some items will have a larger impact than others. And while we continue to automate and place things on our network for ease of management for our teams, it also makes it easier for the adversaries to access the networks and devices at the same time.

Expert Insights - Jonathan Risto, Community Instructor, SANS. *[cont]*

LU: Cyber-crime is a challenge for all industries, do you think mass transit has been quick enough to focus on solutions?

JR: All industries need to continue to focus, adapt, and improve their cyber security measures -- and mass transit is no different. The adversaries that we all face have different goals. Some desire financial gain, some just want information/knowledge, and others want to cause a disruption of service. While all may use the similar methods to attempt to get into the network, their targets are different once they are there. There are so many facets to security, and we need to have an understanding of all of them. With one small mistake, the bad guys can gain access to our network. And while we continue to automate and place things on our network for ease of management for our teams, it also makes it easier for the adversaries to access the networks and devices at the same time.

LU: Within the structure of a mass transit agency (rail / metro) who should be taking the lead on digital security?

JR: I feel that there should be a senior person dedicated to security, and that is the Chief Security Officer (CSO). Depending on the size of the organization, this could even be further refined to the Chief Information Security Officer (CISO). Regardless of the title, the person is the security champion, and should be a senior exec team member and this needs to be someone who is able share and convey the business impact of digital security items, so that they are understood by the complete exec team. Regardless of who is in charge of the structure, everyone, and I do mean everyone, has a part of play in the security of the organization. The employees see so much more than any one security team member is able to, so having employees report when they see strange things, the entire organization becomes the sensor network helping to detect and report things. Proper awareness training is needed to do this, but it greatly increases the security of the organization.

SANS

For more on SANS visit www.sans.org

They can also be found on Stand 18 at the SafeRail Congress, Washington D.C. April 11-12 Doug Wylie, CISSP Director of their Industrials & Infrastructure Portfolio will also be a speaker.

Your rail system... secured

With a layered approach that:

- Embeds security firmware at the network switch level
- Ensures protection against cyber attacks
- Secures the core, the access layers and network service for IoT

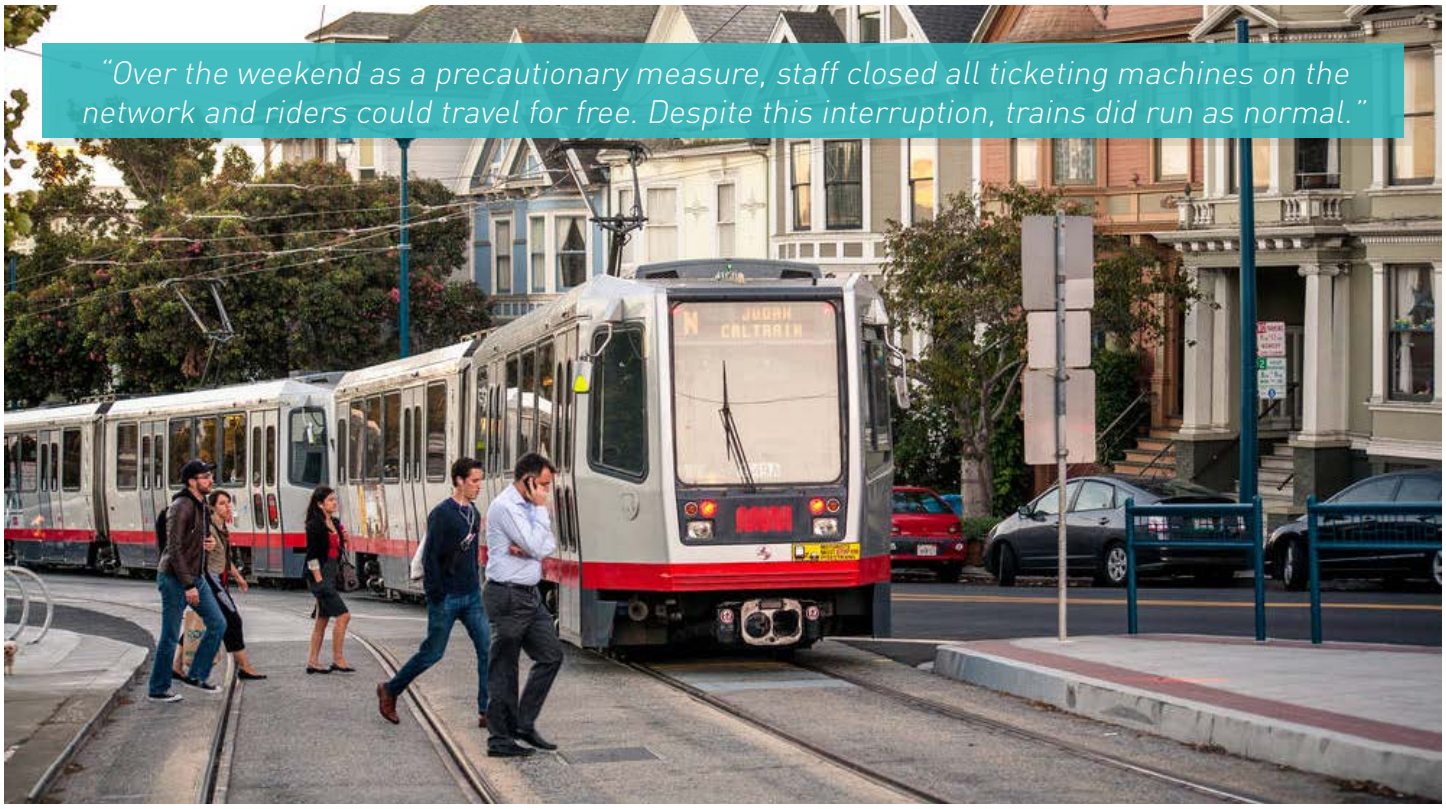
We connect transportation subsystems, with technology that works.
For your people, your passengers, and your services.

enterprise.alcatel-lucent.com/securetransport
transportation@al-enterprise.com

Alcatel·Lucent
Enterprise

Hackers Breached San Francisco's Transit System and demanded a $73,000 ransom.

The computer system that serves San Francisco's bus, light rail and trolley car network was hacked in November 2016, giving locals tens of thousands of free rides on the nation's seventh-largest transit system in the busy post-Thanksgiving period. The ransom according to correspondence between the San Francisco Examiner and the email address displayed on San Francisco's Municipal Transportation Agency (SFMTA) also known as Muni's hacked computer screens. Muni employees' hacked computer screens, was 100 Bitcoin, or about $73,000.



"Over the weekend as a precautionary measure, staff closed all ticketing machines on the network and riders could travel for free. Despite this interruption, trains did run as normal."

The hackers shut down work stations, ticketing machines and computers and attacked the organisation's domain controller and network-attached Windows systems. There are roughly 8,500 computers, Macs and other boxes on the agency's network and **2,112** infected computers displayed a message which read: "You Hacked, ALL Data Encrypted. Contact For key (cryptom27@yandex.com)ID:681 ,Enter".

The cyber-attack began on a Friday, with a demand for a ransom in order to agree to unlock the systems and restore MUNI's services. The hacker or hackers calling themselves 'Andy Saolis' a pseudonym commonly associated with HDDCryptor ransom attacks also provided a list of all 2,112 machines under their control, as well as a Bitcoin wallet where the ransom money could be paid into.

How does this happen? The target machine is commonly infected by accidentally opening a virus in an email or download, this allows the malware to intercept the entire network. The email address suggests that it is a Russian email address and had been linked to other cyber-attacks.

"They give Your Money and everyday Rich more! But they don't Pay for IT Security and using very old system's !" Saolis wrote in an email to Muni staff during the hack.

Over the weekend as a precautionary measure, staff closed all ticketing machines on the network and riders could travel for free. Despite this interruption, trains did run as normal. Muni lost money by giving away free rides over the weekend, but it didn't pay the 100 bitcoins demanded. Instead, by the Sunday evening Muni restored its systems with help from the agency's internal tech team and the ticketing machines were back working. No customer data was lost.

Failure to gather revenue from the busy weekend meant that the transit agency lost $559,000 each day. A statement from SFMTA claimed they'd never considered paying the ransom. The investigation is ongoing with support from the Department of Homeland Security (DHS).

More Than 75% of Crypto Ransomware in 2016 Came From the Russian-Speaking Cybercriminal Underground.

Out of 62 new crypto ransomware families discovered by **Kaspersky Lab** researchers in 2016, at least 47 were developed by Russian-speaking cybercriminals. This is one of the findings of an overview of the Russian-speaking ransomware underground, conducted by Kaspersky Lab researchers. The review also found that small groups with limited capabilities are transforming into large criminal enterprises that have the resources and intent to attack private and corporate targets worldwide.

Crypto ransomware – a type of malware which encrypts its victim's files and demands a ransom in exchange for decryption – is one of the most dangerous types of malware today. According to Kaspersky Lab telemetry, in 2016 more than 1,445,000 users (including businesses) around the globe were attacked by this type of malware. In order to better understand the nature of these attacks, Kaspersky Lab researchers conducted an overview of the Russian-speaking underground community. One of the major conclusions is that the increase in crypto ransomware attacks observed in recent years is the result of a very flexible and user-friendly underground ecosystem, allowing criminals to launch crypto ransomware attack campaigns with almost any level of computer skills and financial resources.

Kaspersky Lab researchers identified three levels of criminal involvement in the ransomware business:

- The creation and update of new ransomware families
- The development and support of affiliate programs distributing ransomware
- The participation in affiliate programs as a partner

The first type of involvement requires a participant to have advanced code-writing skills. The cybercriminals who create new ransomware strains are the most privileged members of the ransomware underground world, as they are the ones who create the key element of the whole ecosystem.

On the second level of the hierarchy, there are the developers of the affiliate programs. These are the criminal communities which – with the help of different additional tools, like exploit kits and malicious spam – deliver the ransomware issued by the malware creators.

The partners of affiliate programs are on the lowest level of the whole system. Utilizing different techniques they help the owners of affiliate programs to distribute the malware in exchange for a share of the ransom received by owners of the program. Only intent, a readiness to conduct illegal actions, and couple of bitcoins are required for participants of affiliate programs to enter this business.

According to Kaspersky Lab estimations, the overall daily revenue of an affiliate program may reach tens or even hundreds of thousand dollars, of which around 60% stays in the criminals' pockets as net profit.

Moreover, during their research into the underground ecosystem and multiple incident response operations, Kaspersky Lab researchers were able to identify several large groups of Russian-speaking criminals specializing in crypto ransomware development and distribution. These groups may unite tens of different partners, each with their own affiliate program, and the list of their targets includes not only ordinary Internet users, but also small and medium-sized companies and even enterprises. Initially targeting Russian and CIS users and entities, these groups are now shifting their attention to companies located in other parts of the world.

"It is hard to say why so many ransomware families have a Russian-speaking origin, but what is more important is that we're now observing their development from small groups with limited capabilities to large criminal enterprises that have resources and the intent to attack more than just Russian targets. We've seen something similar with financial malware groups, like Lurk. They also started with massive attacks on online banking users, and then evolved into sophisticated groups capable of robbing large organizations, like banks. Sun Tzu said: If you know the enemy and know yourself, you need not fear the result of a hundred battles. That's why we've created this overview: ransomware gangs are turning into very powerful enemies, and for the public and the security community, it is really important we learn as much about them as possible." - **said Anton Ivanov, security researcher at Kaspersky Lab,** and the author of the overview.

Read more about how Russian-speaking underground ransomware ecosystem works on **Securelist.com**

Mass Transit Systems embracing 21st Century Transit Policing

Atlanta MARTA · Boston MBTA · Buffalo Niagra NFTA · Charlotte CATS · Dallas DART · Sacramento SACRT · San Francisco BART · Santa Clara VTA · Victor Valley VVTA

ELERTS is the #1 'See Something Say Something' mobile app for transits

HOW?

- Riders use ELERTS mobile app to report safety issues to transit police
- ELERTS app enables 2-way communication between riders and dispatch
- Riders report what they see and hear in real-time to transit police
- Riders send description of incident with photos or video
- GPS location sent with incident report so police know where situation is happening
- Increase security and safety without additional staffing
- Cloud based, no maintenance required
- Supports iPhone and Android phones
- NIMS Compliant
- Simple and easy to use

In a crisis situation, there is no better tool to provide instant information to help quickly resolve an issue

ELERTS 877.256.1971 ▪ elerts.com ▪ sales@elerts.com

Terror train wreck threat from new rail signal system – security specialist.

"We know that the risk [of a cyber-attack] will increase as we continue to roll out digital technology across the network..."

Hackers have the ability to tap into the European Rail Traffic Management System (ERTMS) currently being trialled in the UK and cause havoc according to a leading rail expert. Professor David Stupples told the **BBC** that plans to replace the current system based with a computer based one could leave the rail network exposed to cyber-attacks. Prof. Stupples - an expert in networked electronic and radio systems at City University in London - said if someone hacked into the system they could cause a "nasty accident" or "major disruption". "It's the clever malware [malicious software] that actually alters the way the train will respond," he explained. "So, it will perhaps tell the system the train is slowing down, when it's speeding up."

Network Rail, the owner and operator of most of the UK rail infrastructure which is in charge of the upgrade, acknowledges the threat. "We know that the risk [of a cyber-attack] will increase as we continue to roll out digital technology across the network," a spokesman told the BBC. "We work closely with government, the security services, our partners and suppliers in the rail industry and external cybersecurity specialists to understand the threat to our systems and make sure we have the right controls in place."

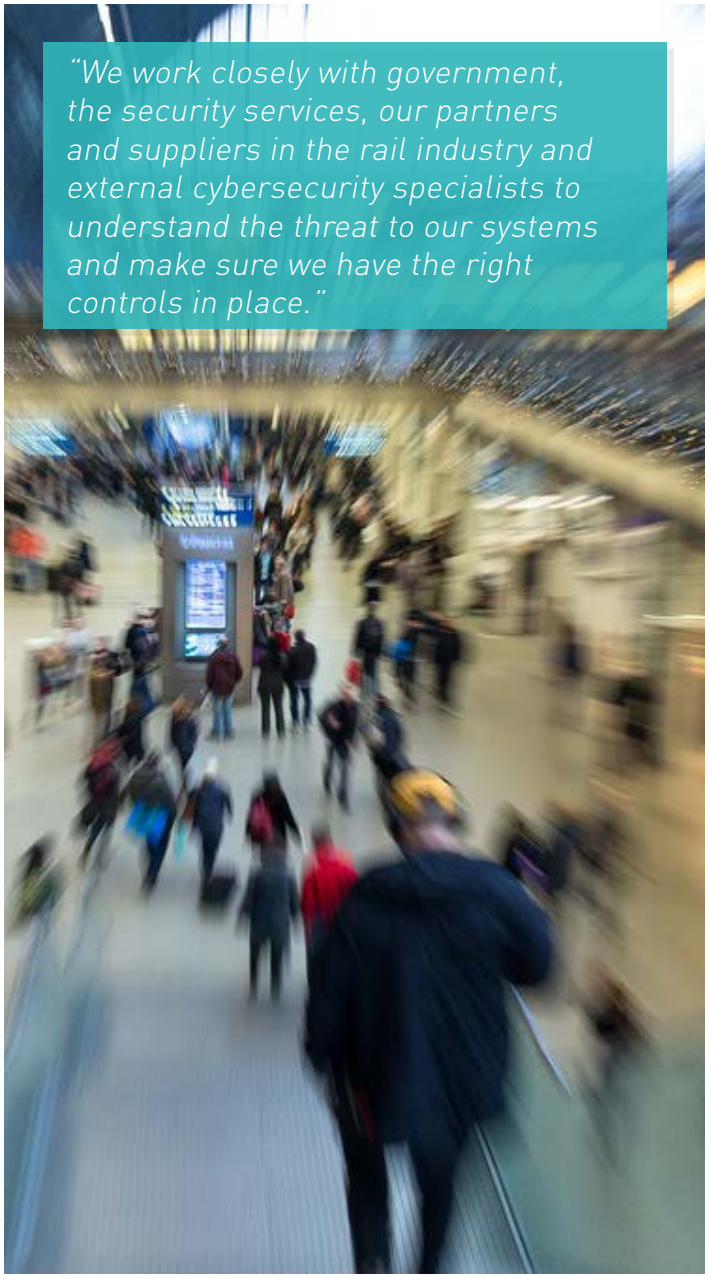
ERTMS (European Rail Traffic Management System) is a signalling and train control system which will replace traditional lineside railway signals with a computer display inside every train cab, reducing the costs of maintaining the railway, improving performance and enhancing safety. There is no history of the system being hacked.

But Prof. Stupples acknowledges the system is well protected against outside attack but is more vulnerable to a rogue rail worker. "The weakness is getting malware into the system by employees. Either because they are dissatisfied or being bribed or coerced," he explained to Richard Westcott, Transport Correspondent for the BBC (**@BBCwestcott**.)

He added that part of the reason that transport systems had not already been hacked as frequently as financial institutions and media organisations was that much of the technology involved was currently too old to be vulnerable. All of that will change in the coming years, as aircraft, cars and trains become progressively more computerised and connected, he concluded.

The rapid advances in the use of digital platforms for control and communication across all aspects of the rail industry have created increasingly integrated security operations but have opened up greater threats from cyber-attacks. These attacks can have the potential to go beyond the electronic domain and cause serious threats to safety and security. One alarming example of this took place in Lodz, in Poland in 2008 when a teenage boy who hacked into the city's tram system used it like "a giant train set", causing chaos and derailing four vehicles.

Reported in the **Telegraph** (UK), Miroslaw Micor, a spokesman for Lodz police, said: "He studied the trams and the tracks for a long time and then built a device that looked like a TV remote control and used it to manoeuvre the trams and the tracks. He had converted the television control into a device capable of controlling all the junctions on the line and wrote in the pages of a school exercise book where the best junctions were to move trams around and what signals to change."



SAFE RAIL

APRIL 11 - 12, 2017
GEORGETOWN UNIVERSITY HOTEL & CONFERENCE CENTER
WASHINGTON DC, USA

MEET 60+
Railroads, Transit Agencies or Government Agencies
*Figure from 2016 event

KEY SPEAKERS INCLUDE:


Art Leahy
Chief Executive Officer
Metrolink SCRRA


Jim Hertwig
Chief Executive Officer
Florida East Coast Railway


Paul Comfort
Chief Executive Officer
MTA Maryland


Skip Elliott
Vice President Public Safety, Health and Environment
CSX


Marc Beaulieu
Chief Transportation & Safety Officer
VIA Rail Canada


Gardner Tabon
Chief, Office of System Safety
NJ Transit


Sean Ryan
Chief Security Officer
MTA Metro North Railroad


John G Anderson
Superintendent of PTC Operations
Canadian Pacific Railway


John O'Grady
Chief Safety Officer,
Toronto Transit Commission


French Thompson
Director, Public Projects and System Design
BNSF Railway

ENSURING MISSION CRITICAL SAFETY AND SECURITY ACROSS THE US RAIL AND TRANSIT NETWORK

2 TRACKS IN 1 CONGRESS

PTC, CBTC, AND OPERATIONAL SAFETY

RAIL SECURITY

"I LEARN MORE IN A NETWORKING COFFEE BREAK AT THE SAFERAIL CONGRESS THAN I DO AT ANY OTHER INDUSTRY EVENT."

STEVE HOOPER, DIRECTOR OF OPERATIONS, PANAMA CANAL RAILWAY

LEAD SPONSORS
ARTESYN EMBEDDED TECHNOLOGIES
LILEE SYSTEMS
WIND AN INTEL COMPANY

WORKSHOP SPONSORS
PROVER TECHNOLOGY
OSIsoft.

CYBERSECURITY PARTNER
WATERFALL Stronger Than Firewalls

ROUNDTABLE SPONSORS
AMA
ELERTS

ASSOCIATE SPONSORS
FRAUSCHER SENSOR TECHNOLOGY

ROUNDTABLE SPONSOR
Rockwell Collins

Visit **www.SafeRailCongress.com** to book your pass

ORGANISED BY GLOBAL TRANSPORT FORUM

SMART RAIL WORLD

Thanks for reading 'Protecting Rail and Metro from Cyber Security Threats'.

SmartRail World Publishing has commissioned the following digital guides for 2017

Keeping Pace with the Demands of the Digital Passenger
(Published 27th January)

Using data to enhance rail and metro operational performance
(Published 7th March)

Protecting Rail and Metro from Cyber Security Threatss

The evolution and future of transit Wireless Communications
(8th May)

The future of signalling & train control
(23rd June)

Rail & Metro Innovation Guide 2018
(18th August)

Creating new revenue streams for rail and metro operators
(20th – 25th October)

To find out more about our digital guides and how you can contribute or partner with them please contact the series Editor Luke Upton on + 44 (0) 20 7045 0946 or Luke.Upton@globaltransportforum.com