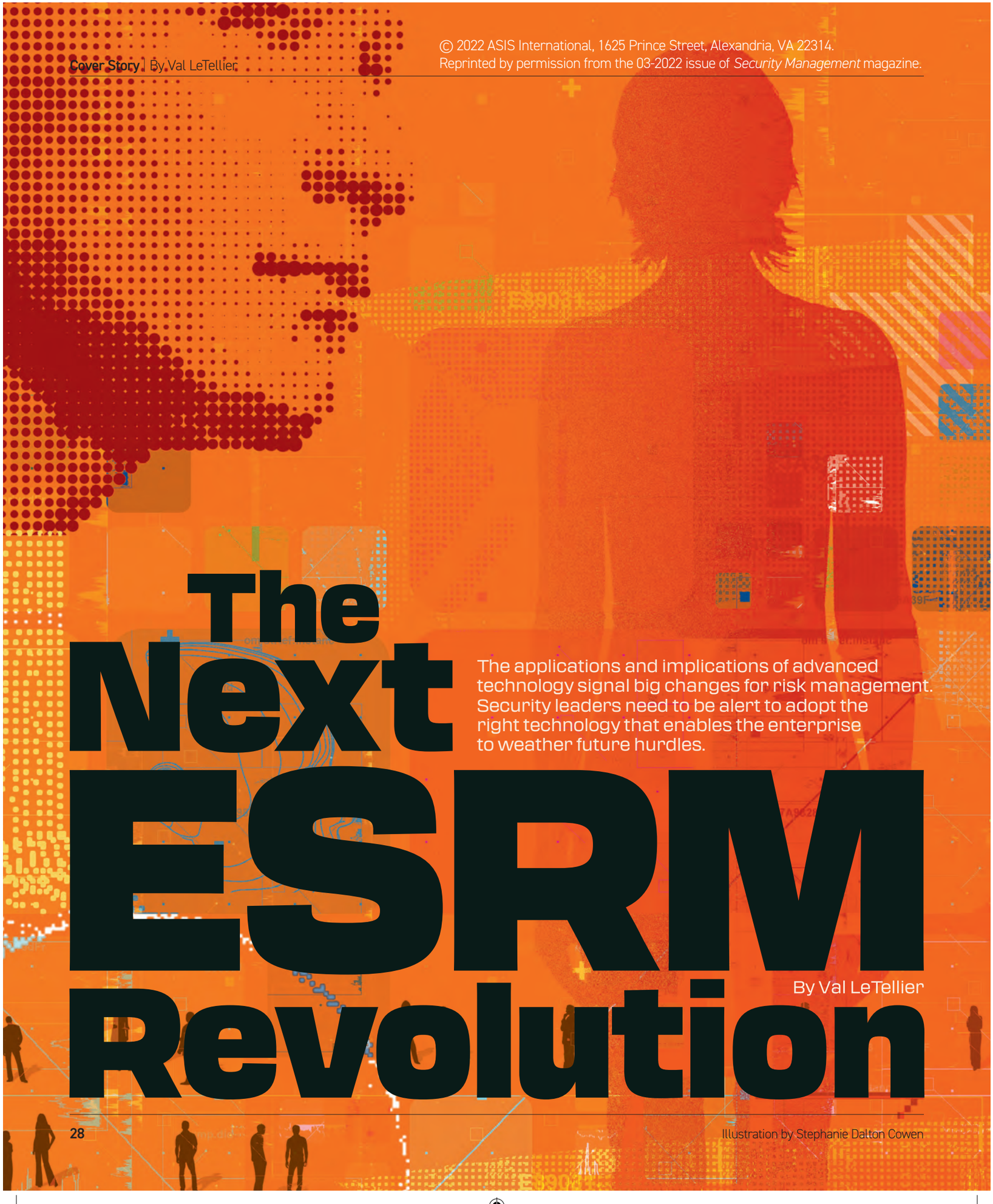

The Next ESRM Revolution

The applications and implications of advanced technology signal big changes for risk management. Security leaders need to be alert to adopt the right technology that enables the enterprise to weather future hurdles.

By Val LeTellier

Illustration by Stephanie Dalton Cowen

The Fourth Industrial Revolution is here.

We live and work in an interconnected world in which machines, devices, sensors, and people connect and communicate with each other. We are surrounded by smartphones, Internet of Things (IoT) devices, location detection technologies, advanced human–machine interfaces, cyber–physical systems, cloud computing, authentication tools, fraud detection measures, smart sensors, advanced analytics capabilities, and digital customer profiling. Smart cities are coming online, with operators able to access enormous sets of information to manage systems.

These technologies are transforming the global industrial landscape, and they are changing enterprise security risk management (ESRM) in ways the security industry is only starting to understand.

Klaus Schwab of the World Economic Forum predicted that the Fourth Industrial Revolution would bring about the "fusion of our physical, our digital, and our biological identities." For security leaders, this fusion is important—it enables multiple surveillance surfaces to monitor, track, and assess behavior in real time.

The result: Ubiquitous and persistent surveillance combined with advanced analytics has created a whole new enterprise risk equation.

New Technologies, New Possibilities

In today's digital world, there is an exponentially growing array of digital sensors that collect massive data pools of information—much of it on individuals and their activities. With the advent of robust data analytics, this bulk information can be enriched by other data sources to create valuable intelligence for risk mitigation and incident investigation.

Some of this data is volunteered by individuals through their use of technology. For example, Facebook boasts more than 2 billion active users per month; its subsidiary Instagram has 800 million monthly users; and Twitter claims more than 330 million monthly active users. All of these users generate data.

In other instances, providers of technology and services collect personal data from consumers and users. Surveillance capitalism in the form of ad-tech sensors collect and track shopping and purchasing behavior, with the data sold to commercial data consumers. Cellular phone networks, DNA mapping, and virus tracking add to the mix. Technological advances like high-speed and high-density 5G cellular networks, ubiquitous IoT infrastructures, and vehicle telemetry provide refined triangulation of an individual's movement.

Other data comes through different channels. One of every two adult Americans are in a law enforcement face recognition network, according to the Georgetown Law Center on Privacy and Technology. The U.S. Government Accountability Office (GAO) has also identified 16 U.S. states that let the FBI use face recognition technology to compare the faces of suspected criminals to driver's license and ID photos.

While these massive data lakes were nominally valuable, it took improvements in data analytics to really make them useful. Machine learning (ML) and artificial intelligence (AI) enabled the aggregation of data sets, the correlation of activity, and real-time and forensic exposure of events.

Fusion technologies have further empowered data analytics by eliminating the spaces between data points and connecting dots that once took days or weeks to link—if they could be connected at all. The fusion is created by a suite of algorithms that churn through public and proprietary records, live sensor feeds, and surveillance archives to identify patterns and connections and allow analysts to draw direct lines between incidents and individuals.

Long gone are the days when people could exist most of the day offline. Now, it's rare to find moments when people are beyond the reach of the sensors surrounding them. The implication of this technological data empowerment is significant for government and corporate security officials; new mechanisms and methodologies are now available to identify and mitigate risk.

A notable example is the FBI investigation into the 6 January 2021 riots at the U.S. Capitol. Federal charging documents show that advanced technologies were employed to identify and prosecute suspects by correlating video surveillance records, facial and gait recognition, license plate readers, cellphone tracking, and online communications. Federal prosecutors have said the investigation is likely to be "one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence."

According to Chuck Wexler, executive director of the Police Executive Research Forum, "If the event happened 20 years ago, it would have been 100 times harder to identify these people, but today it's almost impossible not to leave your footprints somewhere."

Even at the security officer level, there are bespoke applications that enable the monitoring, tracking, and reporting of suspicious activity through real-time streaming of video surveillance feeds. Silicon Valley firm Knightscope, for example, takes this a step further by eliminating the human sensor completely, equipping autonomous security robots with license plate readers, thermal heat sensors, and facial recognition capabilities. Instead, humans are relied on to respond to alerts from the robotic and autonomous sensors.

While near or actual real-time correlation is a game-changer, so is the more nuanced execution of deep dive investigations that find patterns in unstructured data compiled over years and decades through phone, financial, and travel records. To a high degree, technology is dramatically streamlining the investigatory grunt work expended in complex investigations.

Government and corporate security leaders are finding themselves in a complex environment in which real-time and forensic investigations using ubiquitous sensors and advanced analytics are increasingly the norm, and they are realizing the possibilities, caveats, and dangers.

The Good

Arguably, the paramount goal in risk management is to prevent harmful incidents from occurring. Next generation security technology enables exactly that, providing the predictive analytics to make security smarter, efficient, and proactive.

For example, forensic and predictive security methodologies are created by applying advanced analytics to dissembled video surveillance data packets. Recent advancements in end-point computing allow ML and AI processing to be built into video surveillance systems for local execution of automated facial recognition, number plate recognition, patterns, and anomalies, transmitting finished analysis to security operating centers for action.

Technology has also streamlined the cooperation between security leaders and police. Beyond facilitating a quick response to incidents, advanced technology is now a core component of police investigations. Facial recognition helps track suspects, and location tracking leveraging mobile device usage makes it easier to correlate anomalies against technical surveillance. Video of criminal activity is often captured by witnesses or even the criminal themselves, which can then be corroborated by phone records, video surveillance, and personal statements. Such is the case of Matthew Perna, 37, who posted a detailed and lengthy social media video of himself at the U.S. Capitol on 6 January 2021. Within a year he pled guilty to obstruction of Congress, entering a restricted building without lawful authority, and disorderly conduct.

The Bad

No technology is without some drawbacks, particularly emerging and evolving technologies. Data can be maliciously altered, advanced analytics can be inaccurate and even biased, and big data can create even bigger cybersecurity risks.

While altered photos and deepfake videos are well-known, less is known about intentionally manipulated data sets that can often go unidentified and alter findings and conclusions. Machine learning and artificial intelligence are built upon algorithms and models created from sample data sets that may have unrecognized biases, such as facial recognition tools that are trained on predominantly Caucasian faces and are less reliable when detecting people of color.

Additionally, the more stored information an organization has, the greater a target it is for data theft or ransomware attacks. Because the data is often held by others (cloud providers), end users need assurances of security and privacy. Enterprise risk managers tend to rely upon their organization's IT department for this, but given the criticality of this role, it is worth understanding the experience and expertise of these stakeholders.

In addition to the technological risks, there are human resources risks in play. Pandemic-induced remote work will likely remain a big part of enterprise security's challenges. After a period in which business leaders have lost a direct view of their employees, many organizations moved toward digital surveillance to ensure productivity. But as firms adopted digital surveillance in the form of monitoring of email accounts, Web browsing, collaboration tools, and even webcams and keyloggers, many organizations are seeing increasing employee turnover due to potential privacy issues.

As reported in a 2021 VMware study *The Virtual Floorplan: New Rules for a New Era of Work*, approximately 40 percent of companies implementing device monitoring or planning to do so have witnessed either increased or drastically increased employee turnover.

The Ugly

While some employees respond to digital surveillance by finding a new job, others skirt official corporate networks, tools, and safeguards in favor of shadow IT.

The increased use of personal devices for work purposes to evade monitoring tools is rightfully concerning to risk managers, particularly as it is often accompanied by cutting corners and neglecting policies and procedures to save time and effort. A good example is forwarding sensitive data to a personal device or account so it can more easily be edited or printed. By doing so, that information then rests unprotected on a personal device and outside the organization's control—and maybe even outside the employee's control.

Best ESRM Practices

As illustrated above, advancing technologies and methodologies are dramatically changing the way the way we live, particularly in a COVID-19 era. But what does it mean for enterprise security and those who manage it? A lot, given that ESRM requires a holistic view of overall security risk and places the responsibility for security risk management decision-making with the asset owners.

Per ASIS International's guideline on ESRM, the concept sits atop four pillars: holistic risk management, stakeholder partnership, transparency, and governance. It is a risk-based approach to managing security programs based on the concept that you cannot protect what you do not understand. To address your organization's risk, you need to know its mission, needs, and priorities.

Next generation security technology is valuable for achieving ESRM precepts; it can be used to identify and prioritize assets, identify, and qualify risks to those assets and then determine the best way to mitigate those risks.

Holistic risk management. One of the best ways to consider all types of security risk is to make data work for you. Security tools are generating increasing amounts of data, so risk managers have a distinct advantage to transform their roles. Security leaders can better protect their infrastructure by identifying issues and security gaps before an incident occurs. They can leverage this data to become a more integral part of the organizational value chain by the way they collect, transmit, and analyze their data.

Fusion technologies allow risk managers to add new sources of data to correlation engines through new networks of sensors, further enabling organizational risk management, efficiency, and effectiveness—impacting the organization's bottom line.

For example, dashboards can be built to monitor sensors, alert, and then report indicators of potential problems. They can integrate disparate security devices and correlate their unstructured data into a single pane of glass that not only monitors and reports the health and performance of security infrastructure, but also the health and performance of the organization writ large. These software platforms combine security, safety, and productivity data to create a common operating picture that feeds business intelligence directly to the computers and mobile devices of enterprise leaders, enabling smarter decision-making, melding cross-organizational ESRM partnerships, and reinforcing the fact that secure facilities are critical to the organizational bottom line.

Stakeholder partnership. In the ESRM framework, security professionals are trusted partners who advise asset owners and work with others to define and enforce security policy. This approach naturally requires robust communication and data sharing with stakeholders. A game-changing solution to this challenge is harnessing the cloud.

Cloud services provide enterprise security risk managers a way to enhance transparency and accountability. Cloud services enable the uploading of massive data sets for analysis and real-time information sharing with risk stakeholders, allowing them—with the proper permissions and administrative roles—to see the same vulnerabilities, liabilities, and gaps that security managers are citing.

As noted above, applying predictive analytics and machine learning against surveillance data can be valuable to achieving non-security stakeholders' goals, such as enhancing productivity and performance. That said, the introduction of employee monitoring tools must be done in a way to maintain morale and avoid dangerous unintended consequences.

Transparency. Cloud services can enable transparency with stakeholders about the nature of identified risks and efforts to identify, prioritize, and mitigate them. That said, the challenge of leveraging advancing technology while protecting employee privacy is not minor. Monitoring of any type and level can generate the perception that employees are not trusted. As such, while transparency is important, so is trust.

The COVID-19 era has accelerated the move toward greater personal data collection. It also showcased how varied personal points of view can be on a single issue. Risk managers should keep these issues in mind when considering the advanced security technology needed and how to present it to stakeholders.

Transparency is critical to gaining buy-in and protecting privacy, as is evaluating deployment requirements, particularly if the organization is deploying a solution across multiple sites. Some transparency is often legally required, especially in countries under data governance regulations. Advanced analytics can transform business operations and streamline compliance, security, and control harmful events, but it's unlikely that everyone within the organization will singularly see it that way. Communication and outreach are vital.

Governance. ESRM governance should align with overall organizational governance, and a committee should lead risk tolerance discussions to make top-level decisions. Given that these decisions will undoubtably include complex issues like advanced technologies, employee privacy rights, and legal issues, security leaders may need to take the lead in educating the stakeholder team on relevant issues.

First though, enterprise security risk managers need to educate and involve themselves. They need to understand the value and risks that advancing technology brings to organization, in terms of risk identification, qualification, and mitigation, as well as in bottom-line productivity.

These technologies, methodologies, and cultural norms are complex and evolving quickly, so this is no easy task. Risk managers serve themselves well by taking time to stay current and informed.

Mapping the Revolution

Humans have always developed better technologies to help make life easier—upgrading from stone to bronze, from coal to electricity, from railroads to airplanes. As new devices, digital tools, and connectivity advance, academics and researchers see the dawn of the Fourth Industrial Revolution approaching. But how did we get here?

1765
First Industrial Revolution

- Mechanization
- Introduction of the steam engine
- Specialized manufacturing industries (steel, textiles, tools) established

1870
Second Industrial Revolution

- Electricity, gas, and oil
- Mass production scales up manufacturing and drives economies
- Introduction of the internal combustion engine
- Development of communications methods, including telephones

1969
Third Industrial Revolution

- Nuclear energy
- Rise of electronics, telecommunications, and computers
- Automation changes production lines
- Creation of the Internet
- Globalization connects markets and resources

Today
Fourth Industrial Revolution

- Physical–cyber systems
- Robotization
- Big data and analytics
- Artificial intelligence
- Virtual and augmented reality

Technology's ESRM Impact

In the right situation, technology can provide a competitive advantage. As business enablers, ESRM leaders can and should leverage specific aspects of the Fourth Industrial Revolution to help their organizations accomplish their missions. Pursuant to that, several themes stand out.

Data can make ESRM more empowered, efficient, and effective. As the saying goes, data is the new oil. The evolution of analytics has driven business leaders to lead and manage based upon data. If the data is accurate, it can enable informed decision-making—a good thing.

As a business enabler, ESRM needs to employ the same approach. Every access control, fire, and cyber–physical intrusion sensor shares data and builds an increasingly sophisticated and structured data set. This information is extremely valuable for enabling real-time risk mitigation but also identifying patterns and profiles to assess future situations, streamline processes, and reduce human effort.

Cloud-managed AI powered video surveillance systems, edge devices, and 5G networks are disrupting traditional surveillance systems with human analytics, face recognition, and behavioral analytics built directly into the camera using AI chipsets. This edge computing reduces the need for high bandwidth backhaul and storage, facilitating scalability and affordability. It also allows ESRM leaders to place and maintain more sensors, which in turn provides greater data for organizational risk and productivity assessment.

Organizational leadership sees these capabilities in everyday life, and naturally expects their application to security. The wide availability and affordability of advanced technologies once only accessible to wealthy firms has changed the landscape. Now, personal data, advanced analytics, facial recognition, and cloud computing are widely available either as licensed software or as a service.

At varying levels, employees understand what is within the realm of technological possibility because they see it in their daily lives through consumer devices, website tracking, and other services, and they expect to see it in the workplace.

Organizational leaders responsible for profitability have the same perspective, but with more of a focus on efficiency and cost-savings. They expect real-time accountability, which is rarely achievable without advanced technological underpinnings. They also want transparency and to be more involved in enterprise security, even to the point of receiving live feeds from surveillance cameras via smartphone apps to monitor business flows. And because they understand and use cloud computing in their job, they know they can affordably have the insights and accountability they are requesting.

Keeping pace with the rapid evolution and application of these technologies requires a significant dedication of time and effort. While daunting, keeping pace with the most significant advancements in intelligent surveillance, cloud services, and data correlation domains—at least at a high level—is worthwhile. Like in any marathon, once you get behind it's hard to catch up.

As an example, risk managers should understand that the future of video surveillance technology includes data analyzed on-site, reduced server costs, and improved functionality and efficiency enabled by high-bandwidth, high-density 5G networks.

Security risk managers should also understand the legal aspects of fusion technology. In the United States, there are no laws at the national level restricting the blending of data sets to generate information that would require a court order to obtain, but that could change to align with regulations like the EU's General Data Protection Regulation (GDPR). In the meantime, organizations must carefully consider the risk/gain equation of what technology they use and how they use it.

Effective data correlation is critical to the successful use of these technologies. The Fourth Industrial Revolution is creating data at an amazing speed. Every day in 2021, Internet users created 2.5 quintillion bytes of data—adding up to 79 zettabytes of total data created, captured, copied, and consumed globally. That's a huge leap from 15.5 zettabytes in 2015.

In the security world, enormous amounts of streaming data are being created by a wide range of monitoring and surveillance systems. Everything from cybersecurity monitoring, surveillance camera feeds, access control, vehicular reports, power usage/distribution, HVAC, and more are hitting security control centers simultaneously and without interruption.

Regrettably, much of this data is delivered in non-standardized and unstructured formats. So, the trick becomes finding the truly usable data points needed to connect for effective analysis.

Video surveillance is by far the greatest contributor to the security data challenge, particularly when the associated metadata is included. It's this metadata that enables algorithms to find anomalies and draw conclusions that people—and many computers—can't find on their own. It can even identify problems an enterprise may not even know it had.

The key is finding a way to better harness and understand this data for enterprise risk and operational security insight.

ESRM talent requirements have evolved. The experience and expertise required of enterprise risk managers have quickly evolved during the last two decades. At a minimum, managers must be appreciative of the value of technology as applied to threat reduction, security efficiency, and overall effectiveness. They must be tech-savvy, adaptable, and, in some cases, capable of managing a team that is able to fuse disparate data sources for analysis.

The ability to harness advancing technology is no longer a "nice to have" attribute of security professionals—now it's table stakes for entry and promotion.

The Fourth Industrial Revolution is underway. It is up to security and risk leaders to manage its applications to benefit the enterprise. Risk managers who know how—and when—to leverage new technologies will capture leadership roles as their contributions to the organization's big data transformation process positively impact risk management and productivity. ■

Val LeTellier is a former U.S. State Department Diplomatic Security Service special agent and Central Intelligence Agency case officer. He is a member of the ASIS International Defense & Intelligence Community and National Capital Chapter (NCC). LeTellier leads 4thGen, a solutions-oriented consultancy enabling organizations to harness advancing technologies for greater efficiency, effectiveness, and mission success.