FRONTLINE CONTRIBUTIONS ACKNOWLEDGED BY APSA
PAGE 7

EDUCATION PREVIEW FOR GSX 2019 IN CHICAGO
PAGE 10

PROTECTING HOUSES OF WORSHIP FROM HARM
PAGE 14

Canadian Security

THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

Summer 2019

Calming the waters

Vancouver Aquarium's manager of security services Robert Ivanovski tells us why animal welfare is part of the job description

www.canadiansecuritymag.com

Some risks are painfully obvious.

Canadian Security
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT
Volume 41 Number 3

Columns

Departments

Cover image: Lorand Szasz

visit **www.CanadianSecuritymag.com**

Check out the video section of our website for interviews, event highlights and our documentary series Security Insider.

ON CALL

Previewing our CS Honours event, coming Oct. 3

As someone who works in media, I tend to spend quite a lot of time on the phone.

The most gratifying calls I get to make are to those people who are about to receive awards from *Canadian Security*.

Such was the case recently when I called Bob Marentette and Sean Sportun to let them know they had received (respectively) *Canadian Security's* Lifetime Achievement Award and Community Leader Award. It's nice to know you can make someone's day (or week) by simply delivering some good news. In a profession where risk is the stock in trade, positivity and recognition can go a long way.

"When risk is the stock in trade, positivity can go a long way."

I don't remember when I first met Bob, but I'm pretty sure it was close to the beginning of my tenure with *Canadian Security*, which was about a dozen years ago.

Bob was relatively new to the Art Gallery of Hamilton then (he joined in 2005 and is now director of operations), but already had a well-established security career behind him, including senior roles at the Royal Ontario Museum and the Ontario Science Centre. My memories of Bob from those times were through his close association with the Canadian Society for Industrial Security (CSIS). And it was connections fostered through CSIS, along with ASIS International and the Canadian Security Association (CANASA), that I began to find my way through the world of security — I learned it is as much about relationship building as it is about protection.

My call to Bob sparked a few memories for both of us, I think, and I'm looking forward to catching up further as we near our award presentation and gala event on Oct 3 in Toronto. (For details about CS Honours, please visit www.canadiansecuritymag.com/cshonours.)

My second call was to Sean Sportun to let him know that he is the recipient of our 2019 Community Leader Award. Like Bob, I've known Sean for almost the entirety of my tenure at *Canadian Security*. Our first conversation was likely about Security Director of the Year, which we awarded to Sean in 2013. (The cover story on Sean that year was presciently titled "Community man.") In the intervening years, Sean hasn't slowed down. On the contrary, he's taken on more and more projects, whether they are in a professional capacity with his employer Circle K Stores, or his considerable volunteer work with Toronto Crime Stoppers.

I have two more calls to make (for now) and that's to the 2019 winners of the Emerging Leader Award and Security Director of the Year (details coming soon).

I sincerely hope that many people reading this will have an opportunity to attend CS Honours this fall. For those who can't be there in person, our next issue will feature profiles on all the winners. By then I will have made many more calls to those people to find out more about how they work and what they find most gratifying about their security roles and responsibilites. If a measure of that comes through when you read the fall issue, then I'll have done my job too. CS

@SecurityEd

Canadian Security
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

Group Publisher
Paul Grossinger
pgrossinger@annexbusinessmedia.com

Editor
Neil Sutton
nsutton@annexbusinessmedia.com

Associate Editor
Will Mazgay
wmazgay@annexbusinessmedia.com

Art Director
Graham Jeffrey
gjeffrey@annexbusinessmedia.com

Account Coordinator
Kim Rossiter
krossiter@annexbusinessmedia.com

Circulation Manager
Aashish Sharma
asharma@annexbusinessmedia.com
Tel: 416-442-5600 ext. 5206

COO
Scott Jamieson
sjamieson@annexbusinessmedia.com

Editorial and Sales Office
111 Gordon Baker Rd, Suite 400, Toronto,
ON M2H 3R1
(416) 442-5600 • Fax (416) 442-2230
Web Site: www.canadiansecuritymag.com

Canadian Security is the key publication for professional security management in Canada, providing balanced editorial on issues relevant to end users across all industry sectors. Editorial content may, at times, be viewed as controversial but at all times serves to inform and educate readers on topics relevant to their individual and collective growth and interests.

Canadian Security is published four times per year by Annex Business Media.

Publication Mail Agreement #40065710

Printed in Canada
I.S.S.N. 0709-3403

Subscription Rates
Canada: 1 Year $42.00 + HST;
U.S.A. (payable in US dollars): 1 Year $72.00;
International (payable in US dollars): 1 Year $82.50

Circulation
Anita Singh
asingh@annexbusinessmedia.com
Tel: 416-510-5189
Fax: 416-510-6875 or 416-442-2191
111 Gordon Baker Rd, Suite 400, Toronto, ON M2H 3R1

Annex Privacy Officer
Privacy@annexbusinessmedia.com
Tel: 800-668-2384

keep™ by FEENICS

BORN IN THE CLOUD

BACKED BY
MERCURY SECURITY'S OPEN
ARCHITECTURE PLATFORM

BUILT BY
INDUSTRY EXPERTS

DESIGNED BY
CUSTOMERS

THE ONLY CUSTOMIZED **CLOUD-BASED** ENTERPRISE ACCESS CONTROL SOLUTION

As a Mercury Platinum Elite partner, Keep is built upon Mercury's Authentic open hardware platform. Providing customized access control solutions that integrate with industry leading technologies.

www.feenics.com

Feenics

Platinum Partner
MERCURY

GardaWorld, IHS Markit partner for travel security

The phrase “duty of care” has come to enshrine many of the central tenets of the security profession, particularly in regard to the protection of people, property and assets.

Senior members of GardaWorld, the Montreal-based guarding and security services firm, as well as the organization’s partner for data and intelligence analysis, IHS Markit, addressed the topic at the International Economic Forum of the Americas, which was held in Montreal in June.

In an interview with *Canadian Security* following the event, Martin Plante, national director for consulting, investigation and travel security, GardaWorld, described duty of care as “the responsibility that an employer has in relation to their employees … and to take care of them wherever they are around the world.”

Martin Plante, GardaWorld

Growth for GardaWorld

The company, founded in 1995 on an initial investment of $25,000, has grown into a multi-national affair, with more than 92,000 employees operating in 45 countries.

Privately-held GardaWorld has grown significantly through acquisition. The company acquired African security provider KK Security, operating in seven African countries, in 2016. In 2018, it acquired United American Security, a company of 3,600 employees, which operates in 16 U.S. states, and U.K.-based NYA, a crisis management consulting firm. Earlier this year, GardaWorld bought Whelan Security, a U.S. firm with approximately 10,000 employees across 31 states.

In Canada, GardaWorld has also significantly bolstered its residential, commercial and alarm monitoring operations, with several acquisitions in the past year.

Christian Paradis, GardaWorld

Christian Paradis, senior vice-president, strategic development, security services, says the company is built for growth and its founder, Stephan Crétier, is keen on expansion. Paradis says GardaWorld is also in the process of diversification. Aside from its more recent interest in building a monitoring business, the company has invested in risk-based consulting and travel risk services.

Travel partner

In 2018, GardaWorld announced its partnership with IHS Markit, a global research and intelligence firm. GardaWorld’s travel security platform, Crisis24, now incorporates IHS Markit’s risk forecasting and analysis, producing real-time reports for Garda’s clients around the world, which in turn help them prepare for or mitigate potential threats.

IHS Markit’s director of country risk consulting Mike Hartnett, who joined Plante and Paradis as a participant in the “duty of care” roundtable discussion at the International Forum, says his firm began forecasting risk about 15 years ago. The current paradigm of risk prediction and analysis for IHS Markit is one that incorporates all manner of data, including social media and direct reports from its 80 full-time analysts who operate globally.

“Those analysts are from the countries and the regions that they cover,” explains Hartnett. “They speak the language, they understand the business dynamics, the cultural and the social norms. They really provide a unique insight into those countries and how the risk dynamics are changing over time.”

IHS Markit provides a one-year “quantifiable forecast” and a three-year “directional view,” according to Hartnett. “What Garda is doing is using those forward-looking risk forecasts to help provide travel security managers with the ability to look out over the next year to three years, to understand where their travellers are going and to understand how those risk dynamics may be changing.”

For each baseline risk assessment the firm produces for the 211 countries it covers, it also generates “at least two viable alternatives” for that baseline “and then we identify key indicators of change that would lead us to believe that one of some combination of those scenarios would come to fruition,” he says.

IHS Markit works with numerous clients globally to deliver its risk forecasts, but has partnered exclusively with GardaWorld for travel risk advisories.

Whether the world is a “riskier” place than it was a decade ago may be up for debate. “But I think one thing that you can honestly say is it’s a more complex risk environment today,” says Hartnett.

“It’s a wider spectrum of recognized risk impacting companies across strategic, operational and tactical levels. … Then there’s just the diversity of different threat actors out there, including states, non-state actors, criminal organizations, activists.”

He says the concept of “duty of care” has driven the travel security market in the last 10 to 15 years, as organizations look to fulfill their “fiduciary and stewardship responsibilities.”

Moreover, IHS Markit’s own legacy in risk analysis provides it with more than a decade of data that can continue to be mined in the service of mitigating future threats. The company tracks real events back to earlier intelligence, says Hartnett. By understanding these relationships better, IHS Markit can further refine its prediction engines.

Travel security could be seen as a bellwether for the entire security industry — less reactive, more proactive. “That’s where the market has to go,” says Hartnett. “That’s where this partnership [with GardaWorld] is helping to lead in some ways.”

— Neil Sutton

CALENDAR

September 8-12, 2019
GSX
Chicago, Ill.
www.gsx.org

September 11, 2019
Security Canada Atlantic
Moncton, N.B.
www.securitycanada.com

September 18-20, 2019
24th Annual Fraud & Anti-counterfeiting Conference
Toronto, Ont.
www.ksllaw.com

October 3, 2019
CS Honours
Toronto, Ont.
www.canadiansecuritymag.com

October 7-11, 2019
Sector
Toronto, Ont.
www.sector.ca

October 23-24, 2019
Security Canada Central
Toronto, Ont.
www.securitycanada.com

October 25, 2019
Anixter Showcase
Montreal, Que.
www.anixter.com

October 29-30, 2019
Securing New Ground
New York, N.Y.
sng.securityindustry.org

November 20-22, 2019
ISC East
New York, N.Y.
www.isceast.com

December 4-6, 2019
PM Expo
Toronto, Ont.
www.thebuildingsshow.com

December 5, 2019
Focus On Healthcare Security
Toronto, Ont.
www.focusonseries.ca

March 18-20, 2020
ISC West
Las Vegas, Nev.
www.iscwest.com

APSA recognizes frontline contributions to security

The Association of Professional Security Agencies (APSA) Canada honoured two security professionals as part of its annual awards program in Toronto, on June 19.

George Papatsanis of Russell Security Services Inc. (RSSI) was named Guard of the Year, while Andre Lelievre of Commissionaires Ottawa was recognized as Supervisor of the Year.

Andre Lelievre, Commissionaires (left) and George Papatsanis, RSSI

Papatsanis, who has roughly 20 years of experience in the security industry, is an after-hours patrol guard at a golf course in Etobicoke, Ont.

He said in an interview his day-to-day responsibilities include patrols of a very large outdoor space, monitoring and keeping intruders out.

In a letter to the APSA committee, RSSI human resource manager David Beck said Papatsanis was nominated because of his handling of an incident that occurred last June, in which a suspect allegedly involved in a stabbing entered the golf course property covered in blood. According to Beck, Papatsanis notified the police and then detained the individual without the use of any force, de-escalating the situation so that the suspect was calm when the police arrived. “The situation could have been much different had George not shown restraint,” Beck said.

Papatsanis said of the incident, “My mind was racing at that time and I had to think fast and speak to him, get control of him first and not to try to put him down or use any words inappropriate toward him to aggravate him more; it was all about de-escalation.” He said that he advised the suspect against running away or further into the property and told the suspect to sit down and relax.

Papatsanis said he is humbled to receive APSA’s award.

Lelievre joined Commissionaires in 2010 after a 30-year career in the Canadian Armed Forces. He worked as special services mobile supervisor and section supervisor on Parliament Hill before taking on his current position as special services supervisor, where he is in charge of mobile supervisor/patrollers, security patrol and alarm response contracts, short term and on-demand contracts, and special events — including Canada Day and Winterlude.

Lelievre also supervises out of country tasks involving Canadian embassies, and security for the Prime Minister’s Office for overseas trips. He said in an interview, “I’ve got to find the guards, make sure that the guards are trained and they know what to do with the PPS (Parliamentary Protective Service) and the RCMP and all of the people involved on the prime minister’s side. They get their orders from there and I do the flight bookings and work in conjunction with the PMO’s office.”

Commissionaires Ottawa says Lelievre was instrumental in saving the life of a colleague, who he checked up on at home after this individual was a no show at work, with the help of emergency services — the individual was barely breathing but was attended to by paramedics.

For Lelievre, the most rewarding part of the job is, “looking after the wellbeing of the Commissionaires out there… taking care of our people is my No. 1 priority.”

On learning he won the ASPA award, Lelievre said, “I was quite surprised and very thankful for the people who submitted my name. I’m just doing my job to the best of my abilities.”

— Will Mazgay

OpenText exec: Know where your data is

A focused approach to protecting assets, smarter budget allocation and cross-department collaboration are best practices that seem to apply more or less equally to physical and logical security, according to insights from Anthony Di Bello.

Di Bello, vice-president, strategic development for OpenText, was one of the speakers at Enterprise World, the company's user conference, held in Toronto in July. In an interview with *Canadian Security*, Di Bello provided his perspective on approaches to data protection.

Waterloo, Ont.-based OpenText develops enterprise information management software. Di Bello came to OpenText in 2017 when the company acquired Guidance Software, maker of forensic security software, where Di Bello served as senior director of products.

"Where a lot of security vendors are focused on building a better perimeter or securing devices, our ultimate goal is getting the security lens as close to data that should be protected as possible," he said. "We shouldn't be watching the devices, we should be watching the data."

His advice to customers? "Know where the data is, know where it shouldn't be and clean up your enterprise. As a security person, the better I understand where data should be and how it should be used, the more focused I can be in my efforts to secure the enterprise. Otherwise I have to secure everything equally, and there's not enough budget and time in the world to execute on that kind of strategy."

The main stage at Enterprise World, held this July in Toronto (image courtesy OpenText)

These lessons are hitting home for many enterprises, he said. Five or six years ago, there was more of a shotgun approach to IT spending and some enterprises were "just buying everything." Today, it is more focused and more effective. There is also a greater degree of collaboration between departments. Increasingly, everyone is a security professional today, including HR, legal and even PR. "They're really all risk folks," he said. CS

— *Neil Sutton*

WELCOME TO
Security Canada
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION
CANADA'S LARGEST SECURITY SHOW
G4S
SENSTAR

By Neil Sutton

GSX is Chicago bound

ASIS International's annual conference, Global Security Exchange (GSX), returns Sept. 8-12 at McCormick Place in Chicago, Il.

Last year was the "first" GSX (held in Las Vegas, Nev.) following a rebranding of the original ASIS International Seminar and Exhibits conference. The organization recently announced its general session speaker line-up for GSX 2019, including Steve Demetriou, chair and CEO, and Joe Olivarez, vice-president, global security, of Jacobs, a multinational engineering company; General John F. Kelly, U.S. Marine Corps (Ret.); and Tarah Wheeler, cybersecurity policy fellow at New America.

Canadian Security caught up with Ron Rosenbaum, chief global marketing and business development officer, ASIS International, for an update on what else we can expect this year.

Ron Rosenbaum, ASIS International

What were the lessons learned from the "new" GSX last year?
We rebranded our 64-year-old event to demonstrate that it is evolving, and to give it an identity that more accurately speaks to the broader, more global security community. What we've learned is that the industry is actively looking for ways to connect in a learning and networking environment. There is a true need for a community-driven event, highlighted by experiences that blend learning, networking and access to the products and technologies that will help shape the future of the industry. As we continue to evolve, we will closely watch how our participants are interacting with the event to better understand how we can anticipate their needs with new program features.

How does GSX stand apart from other security events?
This year, GSX has more than 300 educational sessions including certification reviews and pre-conference programs. Our Disruption District is right in the exhibit hall with two X Learning Stages offering fresh, forward-thinking TedX style content. The Disruption District features a Startup Sector highlighting new companies with emerging technologies, a Shark Tank style Pitch Competition and presentations from our Innovative Product Awards (IPA) winners. Our D3: Drones, Droids and Defense learning theater returns this year with more live demos and learning opportunities connected to the use of unmanned vehicles in the security field. Our Career HQ offers resumé critiques, mentoring and sessions designed to help attendees elevate their careers. And of course, GSX offers attendees and vendor partners the opportunity to unwind and mingle with peers and customers at a variety of networking and social events.

The "first" GSX, held in Las Vegas, Nev., last year.

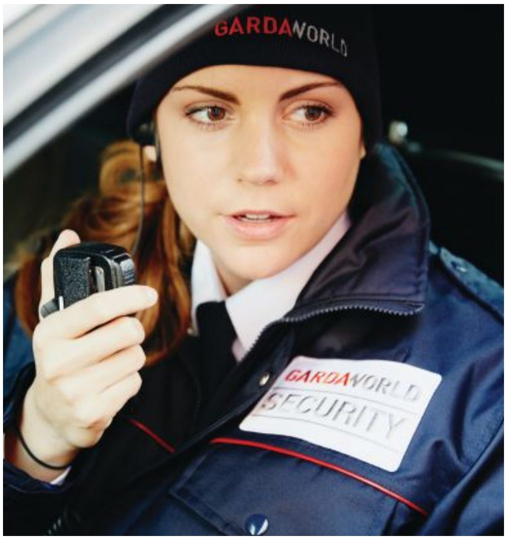
Are there any areas of the GSX education program you would like to highlight for 2019?
New this year are four Game Changer sessions that will address critical topics. A few of the more cutting-edge areas of focus include unmanned systems, cybersecurity, the cannabis industry and workplace violence, to name just a few. There is so much to learn, with so many expert and peer-led presenters, session styles and formats. GSX really is the event that's "By the industry and for the industry!" Our full learning schedule can be found at www.gsx.org.

Did ASIS members request any specific areas of education?
Our members are looking for a wide range of security intelligence…ranging from benchmarking information regarding physical and operational security to insights regarding the latest digital technologies and applications that will help safeguard us for tomorrow. Sessions addressing Enterprise Security Risk Management topics continue to be in high demand. This is being addressed in a variety of formats including a one-day intensive pre-conference program as well as 13 classroom style and X Learning Stage sessions.

We have also had requests from our international members to live stream sessions. We are proud to be in our third year offering Global Access LIVE!, which streams a variety of topics including our general sessions. This allows everyone to access GSX from work or home! Many chapters are viewing them as a group in watch parties! And lastly, our learning lab environment extends from the general session stage to the classroom to exposition floor to the computer screen.

We're truly modernizing our GSX educational offerings so security practitioners can consume critical content where they want it and in the format they prefer. CS

The right resources, in the right place, at the right time



The best range of security services in Canada

- Security guards
- Mobile patrol and alarm response
- Event security
- Executive protection
- Investigations and consulting
- Loss prevention
- Concierge services
- Travel security

GARDAWORLD

TIME TO GROW

Sometimes big concepts like ESRM need breathing room to flourish

During the latter part of June I had the honour of attending the ASIS Board of Directors meeting in Atlanta, Ga.

Before the board meeting, I was also part of the ASIS team that presented an introductory Enterprise Security Risk Management (ESRM) workshop to approximately 40 attendees. It was a great course, full of interesting conversations, opportunities to network with other security professionals, and a chance to create another group of newly-minted ESRM evangelists.

I always enjoy these sessions, spending time with my fellow ESRM instructors and taking security professionals who have never heard of ESRM or a risk-based, business-focused approach to security along a journey of discovery. This session was more special because of one early comment that came to our team.

As a group of instructors, we always do our best to bring those who don't understand how ESRM can create a successful security program slowly down the path of discovery. We've found over the last few years that the best approach is always one of encouragement, helping security professionals realize they are probably using an ESRM approach where they work today, they just didn't realize it.

We received one amazing comment from a recent attendee. I won't share the comment verbatim, but the theme of the comment focused on their reluctance to attend, and the realization of how powerful an ESRM-based approach can be. The attendee was interested in the concept of ESRM, but unsure how well it could be taught or absorbed. They stated they weren't too motivated to attend, but going to Atlanta beat going to another city. They had a preconceived notion that not much could be taught in two days, and were unsure of how to use ESRM within their own organization.

I was pleasantly surprised to read how quickly their mindset changed, and that they truly saw the benefits of an ESRM based security program. They appreciated the efforts of the instructors, and were eager to apply the principles to their own organization. All of that occurred in just two days!

I realize you can't validate a program on just one person's comments, but this attendee summed up many others comments regarding ESRM, and the benefits we can realize as security professionals. Over the past few years I've enjoyed teaching ESRM at GSX for ASIS, and speaking on ESRM topics at a number of conferences and seminars. I do remember there were some dark times, when I didn't think we'd ever embrace ESRM or see how we could change, and become a profession based on risk. I wrote the same thoughts in this column a little while ago, expressing my frustration and concern for our industry, and my misgivings that security folks weren't appreciating the benefits of ESRM.

Time brings change. I see now we're adjusting our perspectives, focusing on security really becoming a business partner able to help organizations achieve their success. I'm seeing this change within my organization and have started teaching my team the principles of ESRM. And I saw the commitment from ASIS regarding ESRM — how this organization is embracing the ESRM philosophy and integrating it into every corner of the business.

I've never been a very patient person! In the past, I would become frustrated with the pace of change, always wanting things to happen sooner than later. As I've matured in both my career and age, I'm now able to appreciate what time can do and to give ESRM more room to grow. I'm glad the industry didn't give up on ESRM either. We're both better for it being around. CS

Tim McCreight is the manager, corporate security (cyber) for The City of Calgary (www.calgary.ca).

FIRST RESPONSE

The speed and content of your reaction to a cyber breach is crucial and may save you some pain

As a cybercrime investigator with the Toronto Police Service, I see the importance of having a complete incident response and recovery plan.

In the wake of a breach, most organizations are concerned with figuring out how the attacker got in, what damage they did, how to get the attacker out, and how they can prevent it from happening again. From a law enforcement perspective, the goal is attribution. We forensically examine the evidence in an effort to ultimately "put the suspect behind the keyboard" and lay criminal charges. Remediation and attribution work hand in hand because they both rely on the same artifacts, known in my world as evidence. A detailed and robust cybersecurity incident response plan can go a long way to ensuring your organization is ready.

1 Know exactly what your systems are logging and how much data you have. While the numbers are coming down, statistics still show that cyber attackers have a foothold in your system for approximately 100 days before they are discovered. The trend is moving away from external notification and more towards internal discovery, yet you don't want to be in a position where you need to rely on your system logs (firewall, access control, intrusion detection, IP video surveillance, etc.) for 90 days of data then realize you only have nine. It is important for both external cybersecurity experts who are helping with remediation and your law enforcement partners who are working towards attribution to have a clear picture of the body of evidence they have to work with.

2 A million events may not mean you have an incident. While this may come across as an over simplification, with a cyber incident plan, it is important to know exactly when the threshold is met to actually execute said plan. Most (I dare say all) corporate networks are being "probed" on an ongoing basis. Each probe, scan and attempted entry is logged as an event. At what point does this mass of events become an actual cyber incident? This is not a question I can answer for you in this column, but it is one you must answer for yourself as an organization. You don't want to trigger your plan and contact the regulators unless you are sure you know what you are dealing with.

3 Part of your plan should be to invest in cyber awareness training for your people and improve their cyber hygiene. Make sure the part of your plan that addresses resiliency testing also tests your people.

4 The greatest harm from a successful cyber-attack is not corrupted data but damaged corporate reputation. Let's take a quick look at just some of the communications outreach that needs to be done during a cyber incident: Media statement; Report to the board; Notice to staff; Notice to customers; Contact regulators; Contact credit reporting; Contact external cyber security; Contact cyber insurance company; Contact (report to) law enforcement. The message in terms of content and timing is key. You don't want to be in a position where the Office of the Privacy Commissioner is contacting you because they got wind of your breach in the media.

5 Businesses are connected to customers, suppliers, service organizations, regulators and more. Don't overlook the security considerations of these connections when developing your plan. In many cases, cyber-attacks are facilitated not directly through your own infrastructure, but through a trusted connection of a known third-party.

Also, pay attention to the technology connecting you to third parties and examine these devices on an ongoing basis from a vulnerability perspective. Equally as important, pay attention to the language in the contracts governing how those connections are used. The wrong wording can shift liability in your direction. Be sure to have trusted legal counsel draft and review these contracts on your behalf.

I have provided five guidelines but I have a bonus thought for you. As a living entity, your cybersecurity plan should receive care and feeding in the form of regular reviews and updates. Your plan should also be vetted by a trusted third party and tested periodically. CS

Kenrick Bagnall is a Detective Constable with the Toronto Police Service Computer Cybercrime Unit (C3) Twitter: @KenrickBagnall.

Free from hate, free from harm

Religious institutions are looking for more effective security options in the wake of violence against their communities

By Will Mazgay

Canada has a reputation abroad and a perception at home of being an open and accepting country. But a shooting at a mosque in Quebec City in January 2017, which claimed six lives, was a painful reminder that violence against religious communities is a threat in Canada.

The danger faced by Muslim institutions was put into sharper focus by horrific violence at mosques in New Zealand this March. Jewish communities meanwhile have been put on edge by recent attacks on synagogues in California and Pittsburgh. For communities at risk of this insidious breed of violence, preparing to mitigate and prevent attacks has become a sad reality, as has dealing with a rise of hate crimes in general.

> "I think the challenge of white nationalism and the growth of far-right militia style groups is a serious security threat."
>
> — *Mustafa Farooq, National Council of Canadian Muslims*

According to Statistics Canada, police-reported hate crime in Canada spiked in 2017 — 2,073 incidents — up 47 per cent over the previous year.

Data for 2018 released this July does show a 13 per cent decrease to 1,798 incidents, but even with the drop, the number of hate crimes in 2018 was higher (with the exception of 2017) than any other year since 2009.

StatCan's data also comes with the caveat that it includes only incidents that are reported, and is dependent on police services' ability to identify hate-motivated crimes. The true numbers and the true extent of the problem remain unknown.

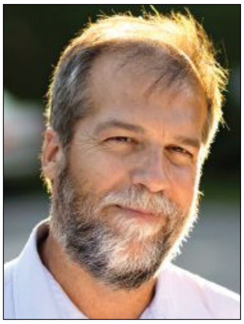
"We know that there's been a pretty sharp uptick of hate incidents and hate crimes against the Muslim community in Canada, and it's something we're paying close attention to monitoring," says Mustafa Farooq, executive director of the National Council of Canadian Muslims (NCCM), a national Muslim advocacy group.

Farooq continues, "I think the challenge of white nationalism and the growth of far-right militia style groups is a serious security threat that many Muslim Canadians, and not just Muslim Canadians but Jewish organizations and Sikh organizations and many others are concerned about."

Ryan Hartman of the Centre for Israel and Jewish Affairs (CIJA), a national Jewish advocacy group, says that the threat level is currently low for Canadian Jewish people, but "the trends that we are monitoring are demonstrating an uptick in nefarious activity targeted towards the Jewish community."

Right-wing extremism is also on the Canadian government's radar. In late June — for the first time — it placed two right-wing extremist groups on its national list of terrorist organizations: Blood & Honour and Combat 18.

Phil Gurski, president and CEO of Borealis Threat and Risk Consulting, is a former CSIS analyst with expertise in terrorism. He sees the threat from white nationalists in Canada mostly coming in the form of "intimidation and bullying," and says that we haven't experienced the level of violence seen in the U.S. or certain European countries — and probably won't any time soon. However, Gurski says the far right does pose a violent threat to Canada, and that the threat can always get bigger.



Phil Gurski, Borealis Threat and Risk Consulting

Better practices

When it comes to guarding against violent expressions of white nationalism and other forms of hate, Farooq says NCCM takes an active role. "We're often reaching out to mosques. We have a community safety guidebook, which we provide to mosques to help them figure out best practices, to ensure safety," he says.

The guide book, beyond advocating for a proactive approach to safety — which includes reporting suspicious activity and hate incidents to law enforcement immediately — lays out some tips for improving mosque security: securing doors and windows; trimming heavy exterior vegetation that attackers may hide in; installing floodlights, alarm systems and security cameras; developing lockdown procedures; posting members of the congregation at entrances during prayer times; and requesting additional police patrols.

NCCM's Farooq says working with local police services can be particularly helpful: "many of whom I'm sure are more than comfortable to come in and provide recommendations about the best ways to keep places safe."

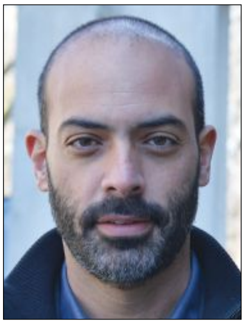
Hamilton Police Service, for example, offers CPTED (crime prevention through environmental design) audits for free to the community. CPTED involves three basic principles: natural surveillance, allowing criminals to be easily observed; access control, creating real and perceived barriers to entry; and territorial reinforcement, defining private, semi-public and public space.

Paul Corrigan, sergeant in charge of Hamilton Police's Hate Crime and Extremism unit, says, "We would get our guys to come out and do a complete look around the whole building first." The CPTED team would then potentially make recommendations for changes, such as how parking can be better organized, along with suggesting erecting barriers to open, vulnerable areas.

The National Community Security Program offers trauma and first-aid training

However, Corrigan also recommends institutions reach out to the private sector as well. "Those people can advise them in ways that we can't," he says.

Adam Cohen, founder and CEO of Montreal-based security consultancy Perceptage — which offers services to a diversity of religious institutions — says that for organizations looking to improve security, they need to make use of their own people. He explains, "The only way to harden a place without making it look unwelcoming and uninviting is by using your own internal resources. That's also the only way to bring down costs. I don't know of many small street corner churches, mosques or synagogues that can fund security guards 365 days a year."



Adam Cohen, Perceptage

Also, Cohen says that security guards don't know the communities they are protecting. "But an usher or greeter is usually someone who grew up within that congregation. He knows his community. He knows his environment," he says. Cohen explains that a person who looks suspicious to a guard may be a trusted congregate, while someone who looks innocuous to the same guard could be a known troublemaker. "So, I always tell institutions, 'you can afford security guards, good for you, put them at the door, but always accompanied by one of your own.'"

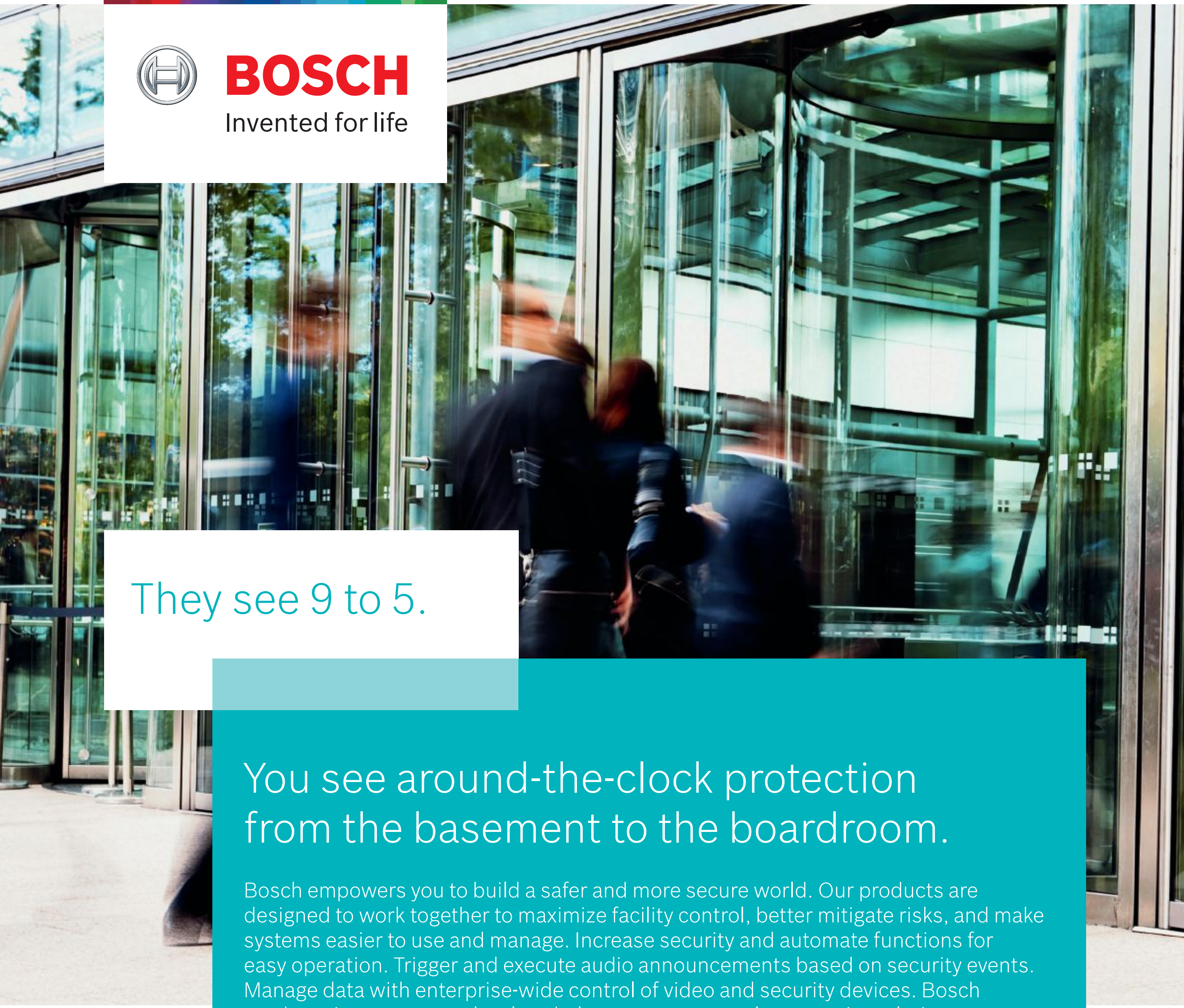
> "We're in constant contact with the leaders in these communities to say, anything you want, just let us know."
>
> — *Paul Corrigan, Hamilton Police Service*

Cohen also warns institutions not to fall into the trap of racial profiling. "You're doing yourself a disservice. By having a certain fantasy of what your enemy looks like, you don't see other threats that don't look like what you imagine them to be," he says.

Improving infrastructure

Beyond observing smarter protocols, for institutions looking to beef up security there are government resources available, notably the Security Infrastructure Program (SIP). This federal program run by Public Safety Canada provides funding — 50 per cent of total project costs to a maximum of $100,000 per project — for non-profit institutions deemed at risk of hate crime. Funding can be used on lighting, fencing, video surveillance, doors, windows, window bars, emergency automated phone systems, intercom and public address systems, panic buttons, and fire detection systems.

Congregation Shaar Hashomayim, a Montreal Jewish community centre and synagogue, recently used SIP funds to improve surveillance. The organization's chief financial officer, Eric Amar, says, "We installed high-resolution digital cameras throughout the organization… We already had external cameras, now



BOSCH
BOSCH

we have internal cameras also, so we have eyes throughout the organization to see what's going on, and we have digital security." He explains that before the SIP grant, "We had analogue technology which was some seven, eight years old, and we changed, and we're looking to stay head of the curve." Amar continues, "People feel a lot more secure."

"This program (SIP) has proven an extremely valuable resource for the Jewish community and other at-risk communities," says Steve McDonald, CIJA's director of policy and strategic communications. "But, at the time the program was originally established (2011), the threat landscape was entirely different. Community institutions that were once primarily concerned with hate vandalism and arson are now exploring the need for lockdown procedures and active shooter training." He explains that the government has been responsive to needed changes over the years by expanding the SIP's budget, broadening the list of equipment and infrastructure that can be funded and, as of this spring, providing up to $10,000 for emergency training for staff, which McDonald calls "life-saving."

> "The only way to harden a place without making it look unwelcoming and uninviting is by using your own internal resources."
>
> — *Adam Cohen, Perceptage*

The CIJA provides free security training with its own program, in partnership with the Jewish Federations of Canada. The National Community Security Program (NCSP) teaches synagogues and other Jewish institutions lockdown procedures, identifying security vulnerabilities, recognizing and reporting threats, recognizing and responding to explosives, and trauma first aid. CIJA's Hartman, who is the director of NCSP, says the training builds confidence and self-reliance for volunteers and staff at institutions.

The NCSP also conducts security audits and supports Jewish organizations seeking SIP grants.

Perceptage's Cohen assists with SIP grants as well, along with requests for proposals (RFPs) for technology, helping institutions discern the difference between technology at different price points and pick out the best contractors.

Cohen says when it comes to purchasing and integrating technology, being smart about how it is installed and used is essential. He explains that cameras won't help if they are in ineffective places — too high to capture faces for example, or in the glow of a streetlamp — and they won't have any deterrent effect if they aren't monitored 24/7.

The security expert also advocates cheaper options when expensive solutions aren't necessary, arguing that locks and motion sensors, available at most hardware stores, are incredibly effective.

In particular, institutions shouldn't underestimate the power of a locked door, says Cohen, who explains that in active shooter events, attackers are trying to do as much damage as possible as quickly as possible, and aren't likely to waste time breaking down a door. "It's just to be able to delay this person and make them leave wherever you are," he says.

To prepare for active shooters, Cohen's lockdown training starts with an assessment of whether doors and windows are secure enough, and whether there are enough safe rooms in an institution. He says, "I always tell the leaders of those institutions, 'Don't let me come and talk to your staff about active shooter and lockdown before you fix those problems.'" To further address lockdowns, "inside, put some sort of mass notification system, a pre-recorded message — something that will allow a person on the inside to press a button and then a mass notification system tells people, we're going to lock down," Cohen says, noting that training members of the congregation to guide people to safe places is critical too.

Amar says at Congregation Shaar Hashomayim, staff security training — that they carry out with the help of a consultant — is their top priority. "You can never be lax about it," he says.

Establishing partnerships

While having smart security practices and effective training and technology can better prepare religious institutions for threats ranging from harassment and vandalism to the unthinkable, building strong partnerships is also an important piece of the puzzle.

Hamilton Police's Corrigan says his service has very good relationships with the various religious communities in the diverse Ontario city. "We're in constant contact with the leaders in these communities to say, anything you want, just let us know," he says. Corrigan explains further that they will automatically step up patrols for religious sites during holidays, special events and busy prayer times, as well as ensure officers get out of their cars and physically check on institutions. "They get up and engage with the people and it makes people feel safer," he says.

NCCM's Farooq says that neighbouring religious institutions of other faiths can also help with collective security. "Working with other community organizations like your local synagogue, like your local temple, like your local church, about sharing best practices, is important."

Amar agrees, explaining that cross-faith co-operation is important for his organization. "We want to share experiences, good ones, bad ones, learning whatever we need to learn from each other's mistakes and each other's successes, so we share information very openly," he says.

Farooq says that at-risk communities can find support from the rest of their neighbours too.

He uses the example of a recent rash of vandalism at a mosque in Owen Sound, Ont. He says, "The community of folks in Owen Sound really stepped up to protect the mosque and protect their Muslim neighbours. That's the kind of thing we know the vast majority of Canadians want to do, to stand up for everybody, and ensure our country stays safe for everybody." CS

Q&A

Robert Ivanovski

Manager, security services,
Vancouver Aquarium

Image courtesy Vancouver Aquarium

Robert Ivanovski moved to Vancouver from Macedonia in 2007. Looking for work, he responded to a community centre advertisement for security guard jobs and started working in a guard position at a public library in downtown Vancouver.

"One thing led to another…" says Ivanovski. He joined the Vancouver Aquarium as a guard in 2010 and there he began to see security more as a career than just a job. "After I got promoted to security supervisor, I started thinking, maybe there is more to this."

He was appointed manager, security services in 2015 and his department has steadily made changes to the aquarium to improve its security profile. The facility's CCTV system has grown from 40 cameras to almost 80, with plans to install more. In recent months, he began hosting lunch and learn sessions to engage all staff in security best practices. *Canadian Security* recently spoke to Ivanovski to find out more.

Canadian Security: **What were some of your priorities when you took on a senior security position at the aquarium?**
Robert Ivanovski: The first year was really a learning experience. The aquarium is all about sustainability and conservation. One of the first things I tried to do was to find ways in which we, as a security department, can contribute in that direction. We started taking better care of lighting management, and in that way we contributed to energy conservation. We got engaged in shoreline clean-ups, which was one of the first green initiatives that came from the aquarium. At the same time, I started improving the existing intrusion system and upgrading the CCTV — not just in the aquarium but in the other satellite facilities, like the Marine Mammal Rescue Centre, for example.

CS: **Is there anything unique to security in a facility like an aquarium?**
RI: I think we pretty much do everything other security [departments] do, with a few distinctions. For example, all our security guards are currently [certified] to First Aid Level 2 — half of us are Level 3 and by the end of next year, we are all going to be Level 3 certified. Different provinces have different certifications when it comes to first aid. Just to give you a comparison, we are just a degree lower than emergency medical responders. We attend dive emergencies, for example. We have a dive specialist. We also have volunteer divers. We have a very specific procedure when it comes to diving emergencies. We are first on the scene, we administer the initial treatment. We notify 911 and let them know it's a diving emergency. We also have specific instructions to notify Vancouver General Hospital of an incoming patient with dive-related injuries, so they prepare the hyperbaric unit and they prepare everything they need for an injured diver. That way, we can save precious time.

We are trained in confined spaces. Next week, we are being certified in IDLH, which is immediately dangerous to life and health training. We need this training because our engineers work in a confined space every day. In case of an emergency, we are trained to do an extraction of an injured worker from a confined space… instead of waiting for the firefighters and ambulance to do that. We save time, and time in such emergencies is critical.

CS: **Do you have to do anything outside the scope of the security department?**
RI: On top of our regular security checks and patrols, we do animal checks during the afternoon and night shifts. All guards are trained to do these observations — we are looking for basically any unusual animal behaviour. If we see any abnormal behaviour, we notify the animal care staff and in the morning we provide them with the report of our observations. Usually in the report, we include if they were sleeping or not, because that may affect their behaviour during the day.

We also check the water levels. All that goes into the report at the end of the night. The [security] training for that is provided by the aquarium. Usually the animal care team will let us know if they notice something… "Just keep an eye on this animal." And we take over after that.

CS: **Tell us more about your latest security awareness programs.**
RI: Everything started with the first security awareness week that I started in February. I wanted to educate the

staff about the importance of security awareness. That was the main objective — how they can contribute to the overall security and safety in the facility. It was almost to shift the culture from being kind of shy or complacent to being an integral part of the overall security, where basically everyone is doing their fair share.

I focused on four areas: the importance of wearing an employee badge, the second was situational awareness (basically be aware of your surroundings), the third was be proactive and report any suspicious behaviour to security. The last one was don't be complacent — complacency is the biggest enemy to safety and security.

From the awareness week came the security recognition program where we recognize employees who helped security and contributed to our organization's safety and security. I sent emails with certificates to all the recipients explaining why they were recognized and to their managers and directors. At the end of the year, we are going to invite all employees who were recognized to a lunch and thank them for taking an active role.

CS: How has that program evolved?

RI: After that, I thought, let's plan something bigger. And the emergency month came from that. I wanted to familiarize all the new employees who were coming on board in June to work for the summer to know our procedures and policies. The best way to do that was to organize an emergency awareness month. I basically covered four emergencies. For example, every week had a different team and different activities. The first week was medical emergencies. We did dive emergencies, a couple of first aid drills. We did lunch and learns where we did recognizing cardiac arrests and how to do CPR. Every day, I sent emails with the theme of the week. I invited guest speakers for some of these weeks to talk about specific topics. I also did a quiz, reiterating what the theme of the week is. All those who participated in the quiz were eligible to enter a draw at the end of the week and got lunch vouchers. Also, all the participants from the quizzes were qualified for the main prize at the end of the month.

The second week was earthquake awareness. I invited a guest speaker to give a speech on the importance of preparedness. The third week was deadly assailant week. I did three lunch and learns. The last week was fire safety awareness week. Again, I invited a guest speaker to talk about the importance of fire safety, and I booked fire extinguisher training. It went really, really well and I have lots of good feedback. I think this is going to be a yearly event. CS

Your cybersecurity CHECKLIST

The best practices you should consider implementing on a regular basis to protect your business from potential attackers

By Brent MacLean

Many of us are aware that IT security needs to be taken seriously and be an ongoing priority for all firms.

While no company or individual can be 100 per cent protected from cybersecurity threats, you can implement security best practices within a cybersecurity audit checklist, which can significantly reduce the risk of you becoming a victim of hackers or employee mishap.

KEEP YOUR OPERATING SYSTEMS UPDATED

Whether you run on Microsoft Windows or OS X, your operating system needs to be set for automatic updates. Turning off computers at night or rebooting promotes the installation of updates (as well as cleans out system clutter). System updates are especially important for server operating systems where all patches and updates need be reviewed and updated on a recurring schedule. Your employees need to be reminded to have their smartphones also set to update operating systems automatically.

ANTIVIRUS UPDATES

Firms need to ensure that anti-malware programs are set to check for updates frequently and scan the device(s) on a set schedule in an automated fashion along with any media that is inserted (USB thumb and external hard drives) into a workstation.

STRONG PASSWORD POLICY

IT policies should mandate complex passwords, meaning at least eight characters with a combination of upper and lower case letters, numbers and special characters. Network settings should require personnel to change their passwords four times per year and personnel should not be able to utilize any of the previous 10 passwords.

USE AUTOMATIC SCREEN LOCK

When a workstation or mobile device has been idle for a few minutes, it should be set to automatically lock the screen to keep prying eyes out of the system.

EQUIPMENT TRACKING

Know where your firm's data resides at all times. This includes, not only servers and workstations, but mobile devices, thumb drives, backup systems and cloud locations as well. Firms should strive to limit access to firm resources to only those staff who absolutely need it and have the proper security clearances.

SECURE DEVICES

Any device that contains firm and client data must be physically or digitally secured. On-premise file servers need to be in a locked room/cage and the office should have a security system. Mobile devices need to be locked when not in use and any data drives encrypted.

DISPOSE OF DATA/EQUIPMENT PROPERLY

All physical files and draft documents with personally identifiable information that is no longer needed should be secured and shredded to minimize the risk of dumpster divers accessing taxpayer IDs. Workstations and other mobile equipment used for processing client data should be thoroughly reformatted or the hard drive physically destroyed to minimize the risk of nefarious data recovery.

ENCRYPT BACKUP DATA

Firms should encrypt any backup media that leaves the office and also validate that the backup is complete and usable. Firms should regularly review backup logs for completion and restore files randomly to ensure they will work when they are needed.

MINIMIZE ADMINISTRATOR PRIVILEGES

Allowing workstations to run in administrator mode exposes that machine to more security threats. This can lead to the entire network being infected, so regular work should NOT be done on a computer in administrative mode, which IT should disable by default.

SECURE SEND

Firms should standardize tools that allow for the secure sending and receiving of client files. All personnel should be educated on using the firm's portal or encrypted email solution for any file containing confidential data.

CONNECT SECURELY

The IT team should train personnel how to connect securely to the firm's information resources either by utilizing a VPN (virtual private network) or other secure connection (look for the https: in the web address bar). Staff should be reminded not to do any confidential work on public WiFi and only connect to WiFi for firm work if they are sure it is authentic (by verifying with the SSID/password with the client). Better yet, have them utilize a 4G LTE mobile hotspot or connect through that capability via their smartphone.

PROTECT MOBILE GEAR

While laptops have often been cited as the top mobile theft risk for many firms and other professional services, mandatory passwords and encryption should be extended to smartphones and tablets.

UPDATE IT POLICIES

Firms should review IT/computer usage policies and provide reminder training to employees at least annually for all new and updated policies. Beyond traditional computer and internet usage policies, firms should add wording on BYOD (Bring Your Own Device), remote access, privacy and encryption where appropriate.

EDUCATE EMPLOYEES

Security education is a vital aspect of managing any corporate entity. In addition to reviewing the firm's policies, employees should be educated on current cybersecurity attack methods such as phishing and pharming, and threats including ransomware and social engineering.

EMAIL AWARENESS TRAINING

Personnel need to be reminded to be skeptical of emails they did not expect and are out of character. Staff need to be reminded how to hover over an email link before clicking or to look at email properties to see if the sender's email address matches. They also need to be regularly reminded not to click on or open suspicious attachments. If there are any questions about a link in an email, it is better to go to the website directly by typing the address into a browser than to risk clicking on the link.

SCREEN POTENTIAL EMPLOYEES/CONTRACTORS

Firms should do a thorough background check on all potential employees or contractors before allowing them access to firm resources. With today's internet connectivity and tiny USB storage devices, thousands of files can be covertly copied in minutes without anyone else realizing it and all a hacker needs is for the firm to grant access. Corporations need to be vigilant about employing all necessary security protocols when it pertains to the daily practices of the company's operations.

GREET OFFICE VISITORS

Employees should challenge anyone in the office they don't recognize and provide that person assistance if they have a pre-arranged meeting with a staff member. If the visitor appears suspicious, the employee should notify someone from management or administration immediately (also called employee "shadowing," social engineering or stalking).

OUTSOURCE SECURITY

Hire expertise when implementing firewalls and security-related features such as remote access and wireless routers so that it is properly configured the first time. Chances are your internal IT people have not been exposed to optimum security training or have experience with setting up a new device. External resources can also be called upon to do penetration testing and risk assessments to identify and lock down any system vulnerabilities.

HAVE A BREACH RESPONSE PLAN

You should have a security incident response plan in place wherever there is concern that firm data has been compromised. This would be in a written format that would include educating personnel on how to document the events leading up to the breach discovery, notifying appropriate firm/external IT personnel of the breach so they can take necessary steps to stop it, and developing an internal and external communications plan.

CYBERSECURITY INSURANCE

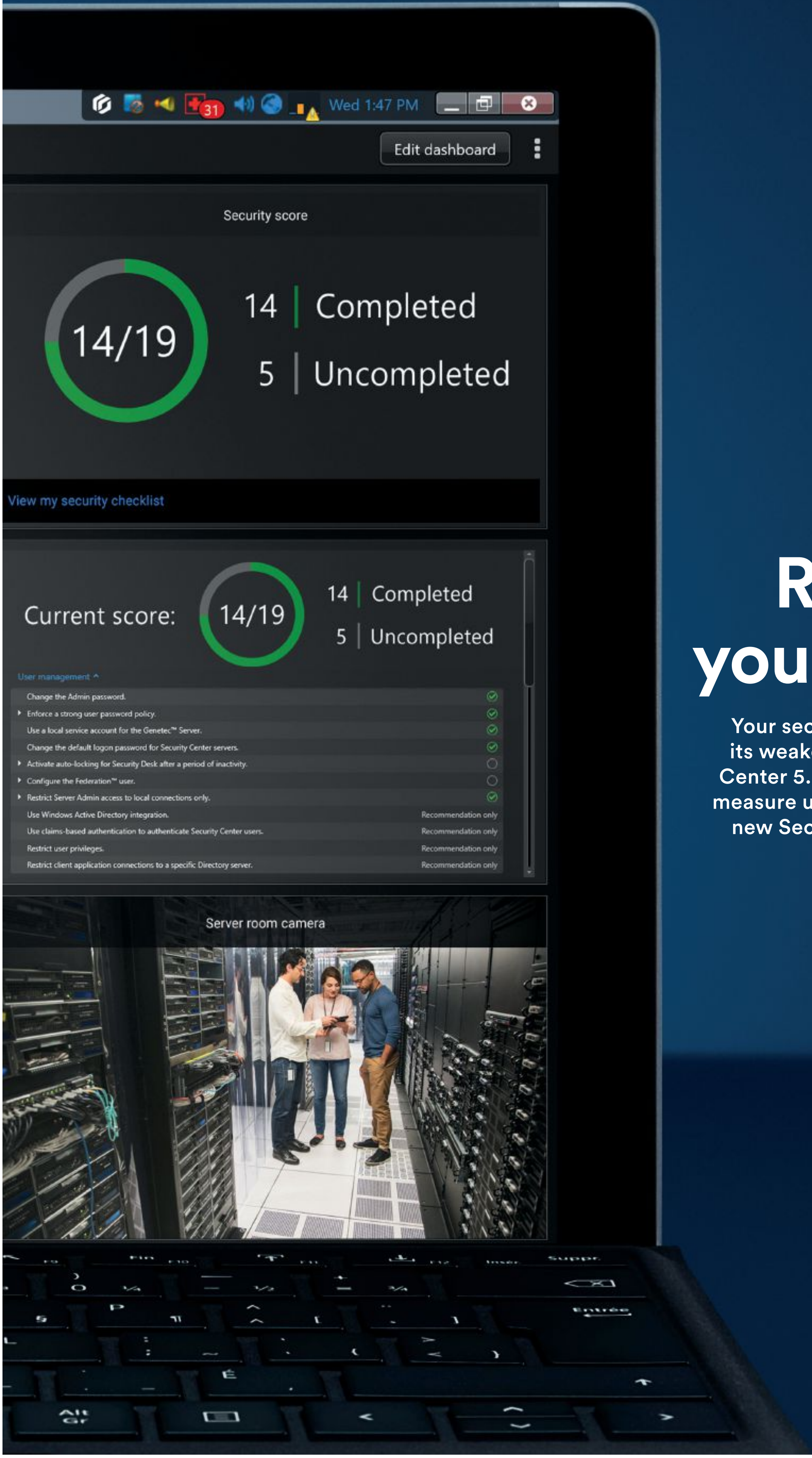
Unfortunately, many firms can do all the right things in regards to information security and still fall victim to a hacker, so to protect against that possibility, they should consider cybersecurity insurance. The cost of this insurance has come down considerably in the last decade and firms should evaluate both first-party insurance to cover the firm's direct losses resulting from the breach (downtime, the re-creation of data, direct remediation costs) and third-party insurance to cover any damages to clients whose data may have been compromised.

DON'T HAVE A CYBERSECURITY AUDIT CHECKLIST YET?

Information security is everyone's responsibility and owners, stakeholders and department heads need to make a concerted effort to educate personnel and follow up on cybersecurity best practices to protect firm and client data.

And, while it's impossible to discuss every possible security scenario within the confines of a single IT article, it is this consultant's viewpoint that employing a strong Cyber Security Audit Checklist like this one, is a good way and a good start to reinforce your most valuable corporate assets and intellectual property. CS

Brent MacLean B.Sc.,M.Sc., is the CEO and senior security engineer at J.B. MacLean Consulting Inc. (jbmconsulting@rogers.com).



Security score

14/19

14 | Completed

5 | Uncompleted

View my security checklist

Current score: 14/19

14 | Completed

5 | Uncompleted

User management ^

Change the Admin password.	✓
Enforce a strong user password policy.	✓
Use a local service account for the Genetec™ Server.	✓
Change the default logon password for Security Center servers.	✓
Activate auto-locking for Security Desk after a period of inactivity.	○
Configure the Federation™ user.	○
Restrict Server Admin access to local connections only.	✓
Use Windows Active Directory integration.	Recommendation only
Use claims-based authentication to authenticate Security Center users.	Recommendation only
Restrict user privileges.	Recommendation only
Restrict client application connections to a specific Directory server.	Recommendation only

Server room camera

Reinforce your resilience

Your security system is only as strong as its weakest link. With Genetec™ Security Center 5.8, understand how your defenses measure up and identify improvements with new Security Score and Firmware Vault.

Genetec™

Find out how to strengthen your security
at genetec.com/SC58

Genetec™ Security Center.

SHARING SECURITY IN CALGARY

City officials and security leaders from municipal and private realms exchange best practices at a Security Executive Council leadership event

By Neil Sutton

Security leaders and their departments are often tasked with rigorous self-examination. Their purpose may be clear, but the means may not. They may have to evolve over time to expand or refine their mandate, add new goals and objectives, or adopt a model (or models) that embraces action over reaction, collaboration over isolation.

Culture change within the security department and its relationship to the larger organization it may serve, was one of the central themes explored during a recent Security Executive Council summit, held this May in Calgary, Alta.

The two-day leadership forum, "Next Generation Security Leader: Driving Current and Future Corporate and Municipal All-hazard Resilience," featured seminars and panel discussions from the City of Calgary's security leadership team, as well as municipal security practitioners from across Canada and the U.S., security leaders in private industry and the SEC's own faculty members. The event's objective, according to the organizers, was to bring together practitioners from both countries, CSOs and CISOs alike, to share proven practices to make communities and companies more resilient.

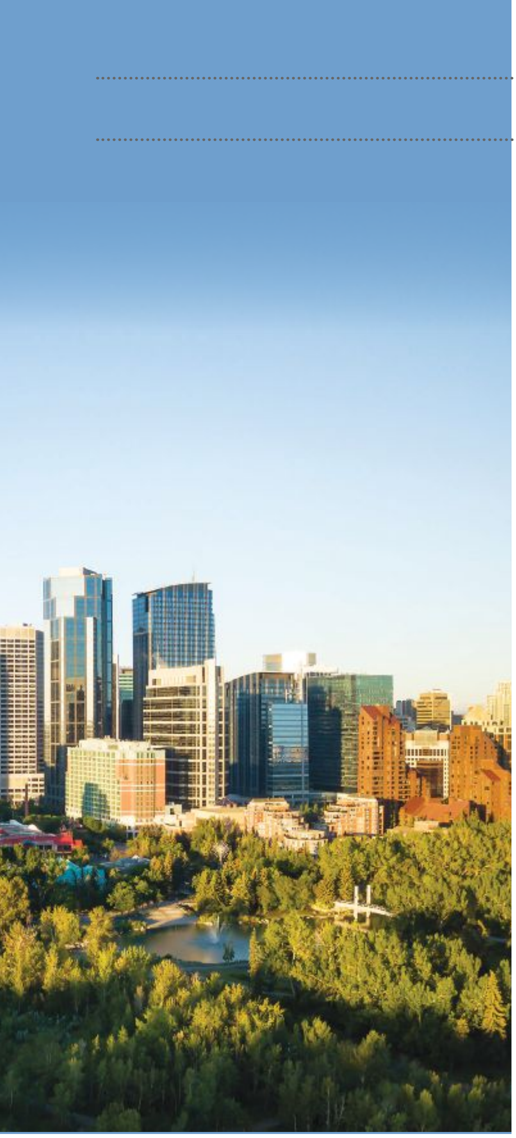
"Security is no longer a solo play, it's a team sport," said Bob Hayes, managing director, SEC, setting the tone for the conference.

"You have to work with all the other groups in the organization," added Hayes. "Whether it's a standards driven or risk driven strategy, if your security program doesn't match the culture, it's not going to work."

Driving culture

Culture change was a central concern for Tony Strickland, head of enterprise security, for therapeutics company CSL Behring, which operates in 35 different countries. Strickland, the first dedicated security leader for the organization, said his team conducted a gap assessment in 2017 to gain a better understanding of where the security department sits in relation to CSL as a whole, and also what the rest of the business expects from his department.

The initial results were concerning. "We were very, very low on the maturity model," said Strickland. On a scale of 1-5, the blended average of returned scores was 0.8. An immediate



turnaround was necessary and the security department actively leaned on other areas of the business to narrow that gap. “That collaboration was critical,” he said. “Those individuals knew they were heard and had a say in things. We got a tremendous amount of traction out of that.”

Making those connections was “huge,” he added. “It really helps us drive culture.” He urged attendees to always stay connected with other departments and strive to answer their questions. “It’s a really strong way for us to create a collaborative environment.”

Every dog has his day

When Tim McCreight, manager of corporate security, cyber, City of Calgary, adopted a rescue dog who had been mistreated, he knew he had his work cut out to win back the animal’s trust. His solution? Become a dog. Relate in a different way and challenge his own perspectives.

“Security is no longer a solo play, it’s a team sport.”

— Bob Hayes, Security Executive Council

McCreight, a speaker at the Calgary conference and a long-time contributor to *Canadian Security* magazine (read his regular column on p.12 of this issue), said he has adopted this change principal in his own work.

“It’s made me realize that throughout our entire careers, if we don’t want to change, we don’t want to adapt, we don’t want to change for the structure and the business that we help to protect, we’re going to fail,” he opined.

A crucial adaptation is to reframe the security department as a business, with business objectives in mind.

“If we don’t start taking a look at ourselves as business owners, we are going to be losing a lot of what I call credence inside the organization,” he said.

“Everything we do as security professionals is to support and enable the business. We don’t run it — it’s not our job. Our job is to support the business by identifying what are the risks against the major objectives, what can we provide for suggestions to remediate and what’s the business going to do to decide.”

One of the most difficult aspects is letting someone else make the decision to accept the risk. But this is central to the security role, said McCreight. “I’m not the CEO. What I am is a trusted advisor… But the business has to decide. And then you have to let them. One of the things we have to do as security professionals is to take our ego out of it. Sometimes business is going to do risky things. We have to let them.”

That last part was the “hardest lesson” he added. Echoing Hayes’ and Strickland’s learned wisdom about the dangers of isolation, McCreight stressed the importance of continuous improvement and communication. “The organization needs to know what we’re going through.”

This is not the military

The final presenter on a three-part panel, Terri Govang, director of technology, Western Canada, at WSP, said, as a consultant, she leans on her previous experience to get the message of culture as an enabler of change across. As such, security cannot operate in a vacuum.

“We have to remember, we’re not a militant culture,” she said. “As security professionals, we can’t just identify risk, put a 10-page report on the table and say, ‘This is how it is.’ It doesn’t work like that.”

Govang pointed to cybersecurity as a natural ally within the organization; she suggested that physical security departments reach out to their digital counterparts to identify common opportunities to help one another. She also said it’s important to talk to sales and marketing departments on a regular basis. Why? Because they can help turn security into a profit centre.

While change is vital, expect some resistance, said Govang. Change can inspire feelings of loss of control. No one likes to be surprised, she said, and successful people may be highly resistant. After all, if they have achieved success with their current methods, why mess with a good thing? “We have to understand what the resistance is and then work through it,” she said. “Some people change when they see the light, others when they feel the heat.”

Another piece of advice from Govang: “Don’t launch and leave.” Management has already had time to become acclimated to change since they are the decision-makers. They have to extend the same courtesy to their employees. “We have to give them a moment to catch up.”

LIVING OFF THE LAND

Derek Manky is chief of security insights & global threat alliances at Fortinet, office of CISO. (www.fortinet.com).

Security risks are often associated with unauthorized downloads of malware or other tools from outside the network that then drive an attack. However, this cat-and-mouse game between technology and threats isn't restricted to how attackers choose their targets. The game continues even after attackers gain initial victory.

Fortinet's latest quarterly global Threat Landscape Report found that attackers are increasingly using tools already pre-installed on targeted systems to carry out their activities. This is known as "living off the land," and enables hackers to hide their attacks behind what appears to be normal, everyday processes, making them more challenging to identify. And because many of these tools include privileged access, they can also be harder to stop.

PowerShell is arguably one of the most popular tools used by IT teams for many reasons. It comes pre-installed on Windows machines and can interact directly with the .NET Framework. It has also become quite popular among cybercriminals. We've tracked adversaries using PowerShell in campaigns to deploy numerous malware, including TrickBot and Emotet banking Trojans. PowerShell, of course, is not the only one. There are other popular utilities that enable attackers to escalate privileges, move laterally across an environment, and install malicious payloads on other systems.

It should be noted that Microsoft in recent years has hardened PowerShell against misuse via measures that restrict the ability to invoke arbitrary Windows APIs, by script block logging, code signing, and support for role-based access administration. But the reality is that attackers can use any language that interacts with .NET, including C#, C++, IronPython, and VB, to accomplish a lot of the same things they can with PowerShell.

As we saw at the start of the year, threats are not likely to abate. Embracing an effective long-term strategy that seeks to address security in an integrated and collaborative fashion is the most important step organizations can take to keep adversaries at bay.

CANADIAN SECURITY HONOURS

CELEBRATING SECURITY EXCELLENCE

Join us for an exclusive awards luncheon to celebrate security professionals in Canada who have made a difference in the world of corporate security.

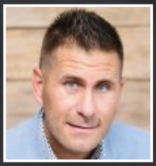
OCT | 3 | 2019

SANDMAN SIGNATURE HOTEL
TORONTO, ON

2019 Awards Include:

- Security Director of the Year
- Emerging Leader Award
- Community Leader Award
- Lifetime Achievement Award

Lifetime Achievement Award
Robert Marentette
Director of Operations
Art Gallery of Hamilton



Community Leader Award
Sean Sportun
Manager, Security and Loss Prevention
Circle K Stores Central Canada Division

☛ **BUY TICKETS**

Presented by
Canadian Security
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

FOR SPONSORSHIP OPPORTUNITIES, CONTACT:
PAUL GROSSINGER | Group Publisher | p 416-510-5240 | c 416-564-2513
pgrossinger@annexbusinessmedia.com

canadiansecuritymag.com/cshonours

PROUD SPONSORS ADT STANLEY Security

4K cameras

Speco Technologies

Speco's 4K Flexible Intensifier Technology Cameras, the O8FB7M & O8FD4M, offer colour in low light, and they are equipped with 4K resolution. The O8FB7M and O8FD4M are designed to fit any lighting application. These cameras have three settings: Colour in low light, monochrome without IR in low light, and monochrome with IR in almost complete darkness. They also come with an included junction box, and feature a five year warranty.

www.specotech.com

Dual-sensor dome camera

Dahua Technology

This Dual-Sensor Dome Camera (DH-IPC-HDBW4231FN-E2-M Series) functions as two individual cameras in one compact indoor/outdoor rated housing. Options include an RJ45 connector with a 2.8mm lens and an M12 D-coded Ethernet connector for an added level of stability in a mobile environment with a 2.8mm or 3.6mm lens. All options include EN 50155 shock and vibration certification. The camera has two independent, 2MP, STARVIS CMOS sensors with dual-stream encoding (per sensor) and the Dahua Intelligent Video System (IVS) analytics, including facial detection. Additional highlights include IR distance of up to 66 feet (20 meters), Basic Starlight Technology for scenes with low-light conditions (0.009 lux), and True Wide Dynamic Range (WDR) at 120 dB for challenging direct sunlight or glare. Power can be supplied via a single Power-over-Ethernet compliant network cable (PoE) or with power from a 12 VDC power supply.

www.dahuasecurity.com

Clear protective cover

Camden Door Controls

Vandal and weather resistant, the low profile CM-CPC1 Clear Protective Cover is designed to protect any Camden flush mount, single gang, door activation device, including push/exit switches keypads and key switches – without limiting the operation of the device. The CM-CPC1 is supplied with a gasket and is suited for both indoor and outdoor use.

CM-CPC1 heavy-duty polycarbonate covers protect single gang door activation devices from rain and snow outdoors and, in harsh indoor environments, protect devices from water, dust and chemicals. They're also a solution in vandal-prone applications, where false activation of a device or damage is anticipated.

www.camdencontrols.com

Siren/strobes

STI

STI's new line of round and rectangular siren/strobes complement the existing Select-Alert mini controller series. The siren/strobes can be used with cabinets, mounted above doors, to the wall, or the ceiling. The Select-Alert Sirens/Strobes are an effective way to alert to unauthorized use, theft or vandalism, as well as unwarranted exits and entries. Features include a round or rectangle shape, and 32 selectable sounds with volume control. The round model (STI-SA5500) has a choice of eight strobe flash patterns with speed selection, and includes a backup battery feature. The rectangle model (STI-SA5600) has a tamperproof lens option. Both models have a 12-24 VDC power supply. Lens choices are amber, green, blue, red, white, or clear (round model only).

www.sti-usa.com

Stainless steel cameras

Oncam

The Evolution 05 and 12 Stainless Steel Camera line features design enhancements that further position the device as a solution for surveillance needs in the most demanding environments. Oncam's Evolution Stainless Steel cameras provide resilient protection in areas where resistance to the elements and compliance to stringent regulations are paramount. The camera enclosure is compact and aesthetically pleasing, making it a solution for applications that feature high-end architecture. In addition to the camera's NSF Certification and IP69K rating, the new design adds more certifications that demonstrate its effectiveness in harsh atmospheres. The cameras also feature a comprehensive range of stainless steel accessories and mounting options. The front cover of the camera can only be opened using a bespoke tool, providing increased safety and protection.

www.oncamgrandeye.com

Video surveillance platform

Genetec

Security Center is an open-architecture platform that unifies video surveillance, access control, automatic licence plate recognition, communications, and analytics. Version 5.8 features customizable live dashboards, enhanced privacy protection, a map-driven mobile app, and functionalities that help users actively monitor the health of their system. Security Center 5.8 enables users to create custom dashboards that will display real-time data, such as video feeds, alarms, reports and charts. Users can set up their dashboards using simple point-and-click tools, and instantly combine data from the entire Genetec portfolio in one screen.

www.genetec.com

AD INDEX

ADT Security Services Canada Inc.	19	dealer.adt.ca	G4S Secure Solutions	2	www.G4S.ca
Avigilon Corporation	32	www.avigilon.com/acc7	Garda Canada Security Corp.	11	www.garda.com
Bosch Security Systems Inc.	17	www.boschsecurity.com	Genetec Information Systems	25	www.genetec.com/SC58
Bull Run Capital	31	www.1stResponderTechnologies.com	GSX	8	www.gsx.org
CANASA	9	www.securitycanada.com	Winsted	21	www.winsted.com/WELS
Commissionaires	23	www.commissionaires.ca			
Feenics	5	www.feenics.com			

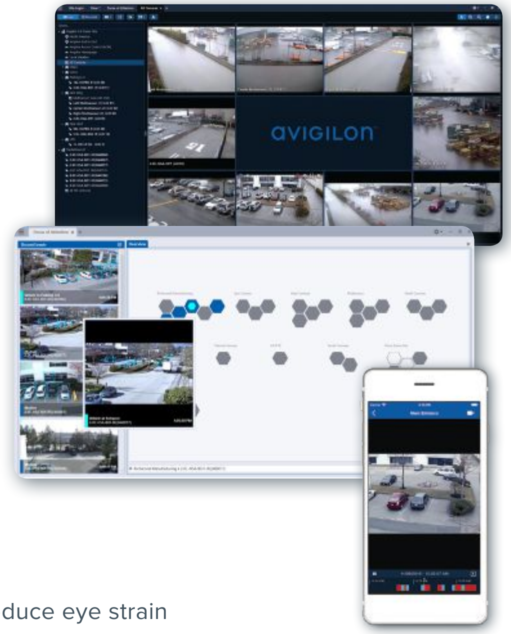
AVIGILON™
a Motorola Solutions Company

A Smarter Way to Monitor Video

Avigilon Control Center 7 Software

Video Surveillance, Transformed

The upcoming release of Avigilon Control Center (ACC) 7, our latest and most advanced version of ACC™ video management software, is designed to revolutionize how users interact with and gain situational awareness from their video surveillance systems.



Focus of Attention Interface

Introducing Focus of Attention — a cutting-edge user interface for live video monitoring that leverages AI and video analytics technologies to determine what information is important and should be presented to security operators.

AI-Powered Analytics

Using our deep learning video analytics and Unusual Motion Detection technologies, ACC 7 software is designed to provide customers with actionable information to help ensure critical events don't go unnoticed.

Dark Mode

ACC 7 software introduces a new theme with colors specifically chosen to reduce eye strain and improve user experience in dark environments, such as video surveillance control rooms.

See the product demo at GSX 2019 – Booth 723
avigilon.com/acc7 | asksales@avigilon.com

Product features and functionalities may not yet be available and, if and when available, may not be as depicted. Images and user interfaces have been simulated for illustrative purposes.