HERJAVEC GROUP

Insights from the

White House Summit on Cybersecurity and Consumer Protection

February 13, 2015

Table of Contents

2014: No Organization is Immune

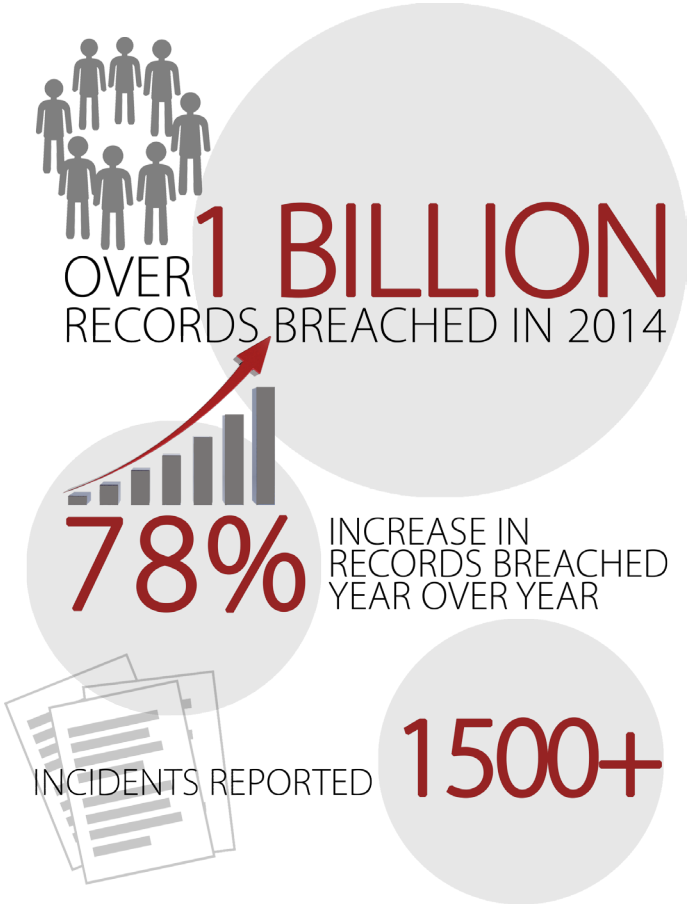
The prevalence of targeted breaches and attacks has raised the profile of cybercrime protection for enterprises worldwide. The FBI has stated that there are two types of firms:

Those that have been hacked & Those that simply do not know it yet.

2014 was labelled as the Year of the Breach as high profile attacks made headlines worldwide:

SONY	**47,000** records stolen	Proprietary Info Employee Details
Anthem Blue Cross	**10,000,000+** records stolen	Names/Birthdates Social Security #s
JPMorganChase	**83,000,000** records stolen	Account Information Small Business Info
The Home Depot	**109,000,000** records stolen	Credit Card Numbers Email Addresses
target	**110,000,000** records stolen	Credit Card Numbers
ebay	**145,000,000** records stolen	Email Addresses Physical Addresses

1.



2.

The statistics show that organizations need a trusted advisor to enhance threat visibility, improve security intelligence & augment staff supporting their environment's perimeter. On February 13, 2015 President Obama invited North America's leading information security experts to join forces with private & public sector executives and government representatives at the **White House Summit on Cybersecurity and Consumer Protection** to discuss opportunities to combat the cyber threats impacting global business and economies.

1. http://www.bloomberg.com/graphics/2014-data-breaches/
2. http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf

Introduction from Robert Herjavec

HERJAVEC GROUP

Friday February 13, 2015:
White House Summit on Cybersecurity and Consumer Protection

On February 13, 2015 President Obama addressed an intimate audience of security professionals at Stanford University for the first White House Summit on Cybersecurity and Consumer Protection. Before signing an executive order promoting private sector cybersecurity information sharing he validated what many of us working in security each and every day know so well: "The very technologies that empower us to do great good can also be used to undermine us and inflict great harm".

Security has become a heightened responsibility of CEOs and board members as business and political battles are waged via computers and malicious code to exfiltrate sensitive data and disrupt the continuity of our organizations. Threat vectors have expanded from routine hacktivists and insiders to Nation States with trillions of dollars in assets and skilled tech savvy recruits intent on successfully breaching their target. The loss of human life resulting from online vulnerabilities is a daunting reality threatening global infrastructures including power grids, transportation systems and health networks. The fact remains – no organization is immune.

Over the course of the full day Summit, President Obama and his staff reinforced the importance of information sharing between private and public sector organizations in the fight against cybercrime. In the spirit of collaboration, Herjavec Group was honoured to be invited to participate in the White House Summit on Cybersecurity and Consumer Protection. I, along with Herjavec Group's VP of Security Remediation Services, Matt Anthony, had the privilege of representing the interests of our firm and our customers at this monumental event.

At the Summit, President Obama called all security professionals and those with a vested interested in data protection for businesses and consumers alike to arms. He highlighted that cybersecurity HAS to be a shared mission. No organization can do it alone. He reinforced that we must work together, as true partners to share appropriate information with one another.

It is in this vein that we ask you to review Herjavec Group's summary of the White House Summit on Cybersecurity and Consumer Protection. Matt and I provided our feedback and insights to provoke questions, start further discussion and most importantly to share our perspectives on this historic event.

To your success,

Robert Herjavec
Founder & CEO, Herjavec Group

Summit Agenda

HERJAVEC GROUP

8:45 AM: Welcome Remarks
Stanford President John Hennessy

8:55 AM: Introductory Remarks
Lisa Monaco, National Security Council

9:05 AM: Introductory Remarks
Jeff Zients, National Economic Council

9:15 AM: Plenary Panel
- Public-Private Collaboration on Cybersecurity
- Kenneth Chenault, Chairman and CEO, American Express
- Anthony Earley, Jr., Chairman and CEO, Pacific Gas & Electric
- Mark McLaughlin, President and CEO, Palo Alto Networks
- Bernard J. Tyson, Chairman and CEO, Kaiser Permanente
- Elizabeth Sherwood-Randall, Deputy Secretary, U.S. Department of Energy

10:00 AM: Plenary Panel
Improving Cybersecurity Practices at Consumer Oriented Businesses and Organizations
- Ajay Banga, President and CEO, MasterCard
- Peter Hancock, President and CEO, AIG
- Renee James, President, Intel
- Brian Moynihan, Chairman and CEO, Bank of America
- Nuala O'Connor, President and CEO, Center for Democracy & Technology

10:45 AM: Remarks
Tim Cook, CEO, Apple

11:10 AM: Keynote Introduction
Stanford President John Hennessy

11:15 AM - 11:45 AM: Presidential Address

1:30 PM: Introduction
George Triantis, Chair, Stanford Cybersecurity Initiative Steering Committee

1:35 PM: Remarks
Administrator Maria Contreras-Sweet, U.S. Small Business Administration

2:15 PM: Plenary Panel
Promoting More Secure Payment Technologies
- John Holdren, Director, White House Office of Science and Technology Policy
- Patricia Falcone, White House Office of Science and Technology Policy
- Aaron Levie, CEO and Co-Founder, Box
- Michelle Zatlyn, Co-Founder, CloudFlare

3:00 PM: Remarks
John Mitchell, Professor of Computer Science and Vice Provost for Online Learning, Stanford University

3:15 PM: Break-Out Sessions
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

---

"These cyber threats are a challenge to our National Security... this is also a matter of public safety... this is also a matter of economic security"

–President Barack Obama

"Appoint Chief Information Risk Officers, not CISOs, reporting to Chief Risk Officers. Get Information Security out of IT"

- Peter Hancock, President and CEO, AIG

"Online Risk Mitigation—it's not the cost of avoiding breaches, it's the cost of staying in business"

– Lisa Monaco, National Security Council

"The cyber world is sort of the Wild, Wild West. And to some degree, we're asked to be the sheriff"

– President Barack Obama

"Cybersecurity is a top priority of the DHS"

-Secretary Jeh Johnson, U.S. Department of Homeland Security

Q&A with Herjavec Group Executive Team

Robert Herjavec, Founder & CEO Herjavec Group
Matt Anthony, VP of Security Remediation Services Herjavec Group

Q: You had the privilege of participating in the White House Summit on Cybersecurity and Consumer Protection – can you tell us what was the event like?

RH: I was blown away by the audience and magnitude of the event. There were secret service members, military personnel, government officials, private sector CEOs. It was an impressive room of approximately 100 guests who were personally invited by the White House. There were two balconies of Stanford students in attendance as well.

MA: What impressed me most was the number of CEOs present. Information Security has absolutely become a board and CEO level issue. We hear it all the time but this was living proof. We were discussing the threat landscape alongside Ajay Banga, President & CEO, MasterCard, Peter Hancock, President & CEO, AIG, and Tim Cook, CEO Apple. These firms didn't send their CISOs or their CIOs to the Summit. These top level executives were aptly discussing the threat landscape in their organizations and sharing their perspectives on the risks in their respective industries.

Q: What about the summit surprised you the most?

MA: The signing of the Executive Order had been well publicized in advance of the summit so that did not take me by surprise. What surprised me was the comfort level of President Obama in discussing malware, adware and the like. I appreciated the level of discussion being had between presentations as it reinforced President Obama's message: Cybersecurity is not an IT problem. It is a challenge for national security, public safety and economic security.

Q: What take aways do you feel our Herjavec Group customers and partners need to know about?

MA: One of the keys for me was the emphasis placed on proactively improving the critical infrastructure of cybersecurity for all firms—whether they be private, public etc. The President promoted the NIST cybersecurity framework and I anticipate all governmental agencies within the US supporting this standardization. At Herjavec Group our consulting and risk management practices also promote a security framework standard for all customers. Despite warnings, some firms choose not to implement a formal protocol and can find themselves challenged without an inventory of their informational assets, contacts and valuable data in the event of a breach. Information security will always be a customized and complicated landscape but the more we can encourage the standardization of a framework, the more open enterprises will be to the discussion.

RH: Ken Chenault from American Express said something that has stuck with me. To paraphrase he said that threats can't be allowed to alter the constancy of his firm's values: trust, service and integrity. I agree with him wholeheartedly. We can't allow ourselves to live and operate businesses in fear. We have to be proactive in our corporate missions and honour the values we set out. I would encourage all of our customers and partners to revisit their security framework as Matt described. It's imperative you have that conversation from the top down to emphasize the importance of security, not as an addition to your organization's values but as a pivotal component to ensuring they are upheld.

Q: Was the importance of insurance tabled at the Summit and how was this sensitive topic discussed?

RH: Herjavec Group has been advocating the importance of security assessments in the world of insurance for some time now. We absolutely foresee the importance of cybersecurity insurance for our enterprise customers and that concern was echoed from private sector firms as well as insurance providers at the Summit. We are constantly reminding customers that the challenge after a breach is that insurance providers will want to understand what "good" looked like prior to the vulnerability being exposed. Peter Hancock (AIG) emphasized that the insurance industry will need to align a framework for evaluation as well as the requirements to be deemed "insurable". He mentioned that cybersecurity is only a tiny fraction of AIG's business today but he anticipates it will grow rapidly.

Robert Herjavec, Founder & CEO Herjavec Group
Matt Anthony, VP of Security Remediation Services Herjavec Group

Q: We've seen rising concern in the health care space with the recent attack on Anthem. Were experts in this field voicing concern at the event?

MA: Absolutely. Bernard J. Tyson, Chairman and CEO of Kaiser Permanente highlighted that "patient information is more important than financial information" during the panel discussion on the Public-Private Collaboration on Cybersecurity.

RH: I couldn't agree more. I recently discussed the Anthem breach with Fortune Live and highlighted that what is most shocking to me, is that a breach of this nature hasn't happened before in the health care space. We are dealing with disparate technology infrastructures and challenging budgets. This heightened risk in health care is because of the importance of personal information (social insurance numbers, medical history etc) in terms of identity theft and prescription theft, but also because of privacy and compliance concerns. Health care is one of the industries that I foresee benefitting most from the degree of information sharing discussed at the Summit.

Q: Any closing comments?

RH: As a techie and security geek, I have to admit, I was a kid in a candy store at this Summit. It was a privilege to be part of this outstanding event and I am grateful to President Obama and his administration for including Herjavec Group in the discussion. This Summit raised the profile of cybersecurity on a global scale and should facilitate further board level discussions about the importance of proactive information security practices.

MA: The White House Summit on Cybersecurity and Consumer Protection allowed me to discuss many challenges that directly impact our customers with industry experts throughout the US. We covered insurance concerns, critical infrastructure security policy standardization, privacy policies—the list goes on. Like Robert, I was in my element and I'm grateful for the opportunity. This interview is one way we plan to share the knowledge gained with a larger audience but I am looking forward to further discussions with our consulting and risk management teams so that we can disseminate our learnings further to our customers directly.

Robert Herjavec, Founder & CEO

A dynamic entrepreneur, Robert has built and sold several IT companies to major players such as AT&T. In 2003 Robert founded Herjavec Group, and it quickly became one of North America's fastest growing technology companies, scaling from $400K in sales to a run rate of $140 million. His inspiring books, "Driven" and "The Will to Win", were simultaneously Top 10 Bestsellers that earned him the title of "Best Selling Author". Robert's motivational business advice has received millions of impressions through TV, print, radio and digital media. He shares his expertise with other entrepreneurs each week as a leading Shark on ABC's Emmy Award-winning hit show Shark Tank.

Connect with Robert Herjavec:

Matt Anthony, VP Security Remediation Services

Matt Anthony is the Vice President of Security Remediation Services at Herjavec Group. Prior to joining Herjavec Group, Matt held numerous leadership positions focused in enterprise security programs, most recently at Alberta Health Services, a $14 billion, 115,000 seat enterprise. Matt has been at the forefront of the information security practice for many years, building and implementing effective programs to govern and manage risk. He has developed and operated Security Operations Centres, led security incident response practices, created policy and governance frameworks, and implemented and operated digital investigation teams.

Connect with Matt Anthony:

Executive Order Signed by President Obama

HERJAVEC
GROUP

At the Summit on February 13, 2015 President Obama signed an executive order directing the creation of new Information Sharing and Analysis Organizations (ISAOs). The ISAOs are intended to share threat information between private and public firms. The information is meant to be disseminated in a standard way so that private organizations and government agencies alike can understand the threats and determine the best course of action to protect their environments.

Herjavec Group partners Palo Alto Networks, and Intel Security, have been tapped to build standards that will support the sharing of information as part of the Cyber Threat Alliance. Additionally, Herjavec Group partner Crowdstrike is creating an ISAO while our partner FireEye is creating an Information Sharing Framework consistent with the ISAO Approach.

Review the complete **Executive Order.**
Watch President Obama's complete **address.**

"This Executive Order supports the transformational shift expected in our industry over the next three to five years. Knowledge of threat actors without information sharing by private sector firms is going to be very unpopular moving forward"

–Matt Anthony, VP Security Remediation Services, Herjavec Group

---

EXECUTIVE ORDER

- - - - - - -

PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, non-profit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive-l (PPD-l) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. Information Sharing and Analysis Organizations. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

Sec. 3. ISAO Standards Organization. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

Sec. 4. Critical Infrastructure Protection Program. (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that appropriate protections for privacy and civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency's activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency's activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

Sec. 6. National Industrial Security Program. Executive Order 12829, as amended, is hereby further amended as follows:

(a) the second paragraph is amended by inserting "the Intelligence Reform and Terrorism Prevention Act of 2004," after "the National Security Act of 1947, as amended,";

(b) Sec. 101(b) is amended to read as follows: "The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order 13526 of December 29, 2009, or any predecessor or successor order, and the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).";

(c) Sec. 102(b) is amended by replacing the first paragraph with: "In consultation with the National Security Advisor, the Director of the Information Security Oversight Office, in accordance with Executive Order 13526 of December 29, 2009, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:";

(d) Sec. 102(c) is amended to read as follows: "Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.), or the authority of the Director of National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, or Executive Order 12333 of December 8, 1981, as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities).";

(e) Sec. 201(a) is amended to read as follows: "The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security, shall issue and maintain a National Industrial Security Program Operating Manual (Manual). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.). The Director of National Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Secretary of Homeland Security shall prescribe and issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program."

Media Summary

HERJAVEC GROUP

globalpost™

The only one way to defend America from these cyber threats is "through government and industry working together, sharing appropriate information as true partners,"

CBS NEWS

Obama's Cybersecurity Plan: Why The Government Alone Can't Protect Us

BBC

"Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this information age"

THE HUFFINGTON POST

Obama signed an executive order aimed at encouraging companies to share more cyber threat data through "information sharing and analysis organizations"

Cybersecurity Threats Call For Better Co-Operation

c|net

Obama signs information-sharing order as privacy question looms

CNN

"It's one of the great paradoxes of our time: the very technologies that enable us to do so much good can undermine us"

The New York Times

"This is a moment to rededicate ourselves and reach out to communities to prevent radicalization"

About Herjavec Group

We Support Your Complete IT Security Lifecycle.

From gap assessment to remediation and incident response,
Herjavec Group is your trusted advisor in information security.

We Consult.

By reviewing your infrastructure's architecture and controls, we identify where your business is most vulnerable to cyber threats and attacks.

We Manage 24.7.365.

We take on the daily operation of securing your environment. Our practice includes flexible on-premise or cloud deployment and management.

We Remediate.

We have extensive practical experience managing complex security breaches. We respond promptly to reduce your recovery time, costs and damage.

At Herjavec Group, we take our role as your trusted advisor in information security very seriously. Information Security Is What We Do. Full Stop.

We are laser focused on protecting the infrastructures of our customers globally and will take every measure possible to learn and engage with security experts worldwide to ensure we remain on the cutting edge of this rising threat landscape.

Dynamic IT entrepreneur Robert Herjavec founded Herjavec Group in 2003, and it quickly became one of North America's fastest-growing technology companies, accelerating from $400K to $140 million in sales annually over 12 years. Herjavec Group delivers managed security services globally supported by a state-of-the-art, PCI compliant Security Operations Centre (SOC), operated 24/7/365 by certified security professionals. This expertise is coupled with a leadership position across a wide range of functions including compliance, risk management & incident response.

Herjavec Group has offices globally including three headquarters in Toronto (Canada), New York City (USA) and Reading (United Kingdom).

For more information, visit **www.herjavecgroup.com**.

Follow Us

Herjavec Group
@HerjavecGroup