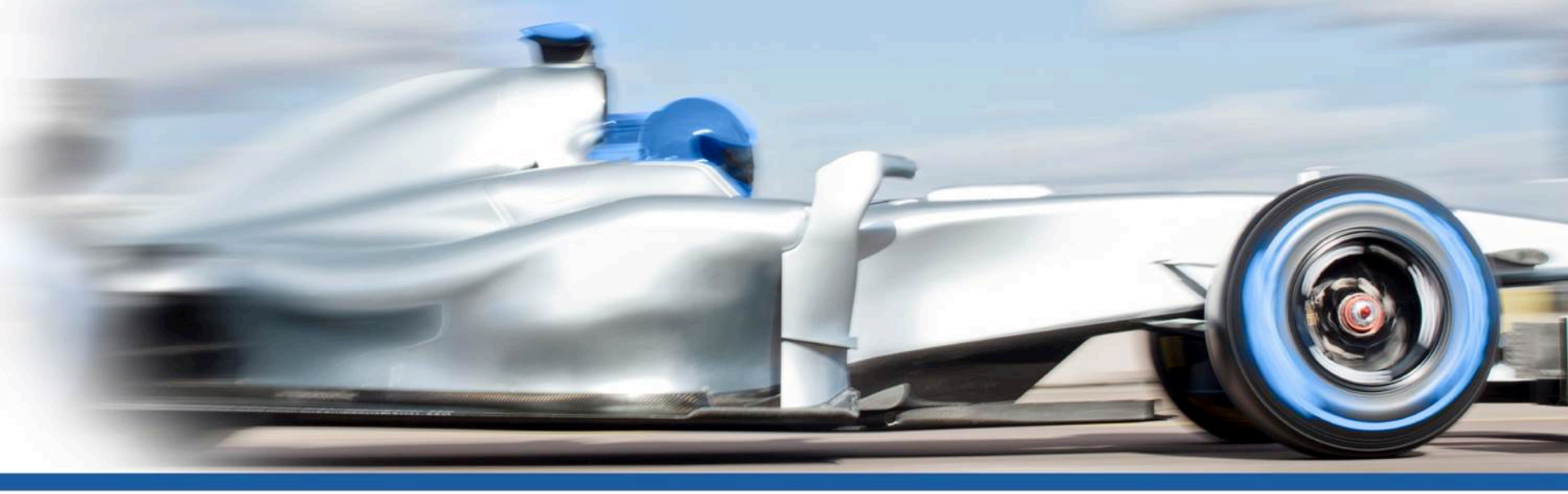


The New IG Playbook for Addressing Digital Age Threats

Navigate with Precision.

DRIVEN

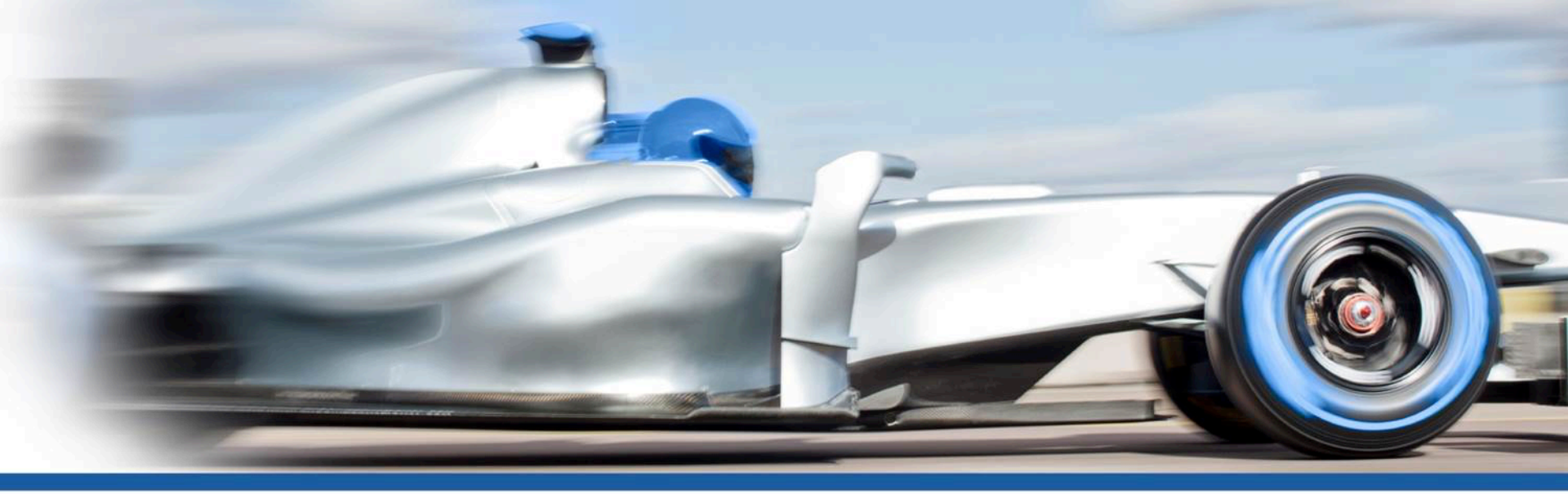
www.driven-inc.com | 1.877.637.4836

Agenda

1. Increasing Risk of Cyberattacks
2. Guidelines from the New IG Playbook
3. Resources
4. Q & A

Hypothetical

- Omega Inc. is a manufacturer that recently developed a unique proprietary technology that could eventually yield billions of dollars in licensing revenue
- Concerned about the effectiveness of its current security measures, Omega IT begins working with legal to shore up weak points across the company's corporate network
- Omega's executive team understands the importance of cybersecurity even though the company previously allocated few (if any) resources to support such initiatives



What are the gateways to cyberattacks on corporate networks?

THE INCREASING RISK OF CYBERATTACKS

Navigate with Precision.

DRIVEN

www.driven-inc.com | 1.877.637.4836

Hypothetical

- Omega has implemented new COPE, BYOD, and BYOC policies to address employee use of smartphones and personal cloud applications
- Omega has also dedicated resources to audit and enforce policies including deployment of MDM software and device monitoring
- Omega is additionally exploring how its email is being managed and whether it should undertake a defensible deletion program for cyber purposes
- Unknown to Omega, many of its employees have taken to using Slack in lieu of email or texts to communicate about work matters

Cyber Threats are Ubiquitous

Gateways to Cyberattacks

- Corporate email
- Web mail
- Social networking applications
- Text messages
- Wikis
- Cloud-based collaboration and messaging applications
- Smartphones and tablets
- Internet of Things
- Personal cloud applications

Cyber Challenges with Corporate Email

"While undoubtedly there will be emails that need to be retained and or stored electronically . . . I am informed by our IT colleagues that our current use of the email system for [storing] virtually everything is not the best way to do this."

Information Governance: Busting Three Big Myths,
IG INITIATIVE BLOG (Aug. 18, 2015)

Smartphones as a Gateway for Cyberattacks

"Mobile phones are considered particularly vulnerable to hackers because consumers typically don't install anti-malware protection onto their devices. . . . some mobile-phone owners unknowingly make their devices vulnerable to attacks when they tamper with operating systems to run unauthorized apps."

***Mobile Bank Heist: Hackers Target Your Phone*, WALL STREET JOURNAL (Aug. 26, 2016).**

Problems with Slack, other Open API Technology

"A surprisingly large number of developers are posting their Slack login credentials to GitHub . . . [which] allows anyone to surreptitiously eavesdrop on their conversations and download proprietary data exchanged over the chat service."

Hacking Slack accounts: As easy as searching GitHub, **ARS TECHNICA (Apr. 28, 2016)**

Personal Clouds: A Hub for Data Theft and Loss

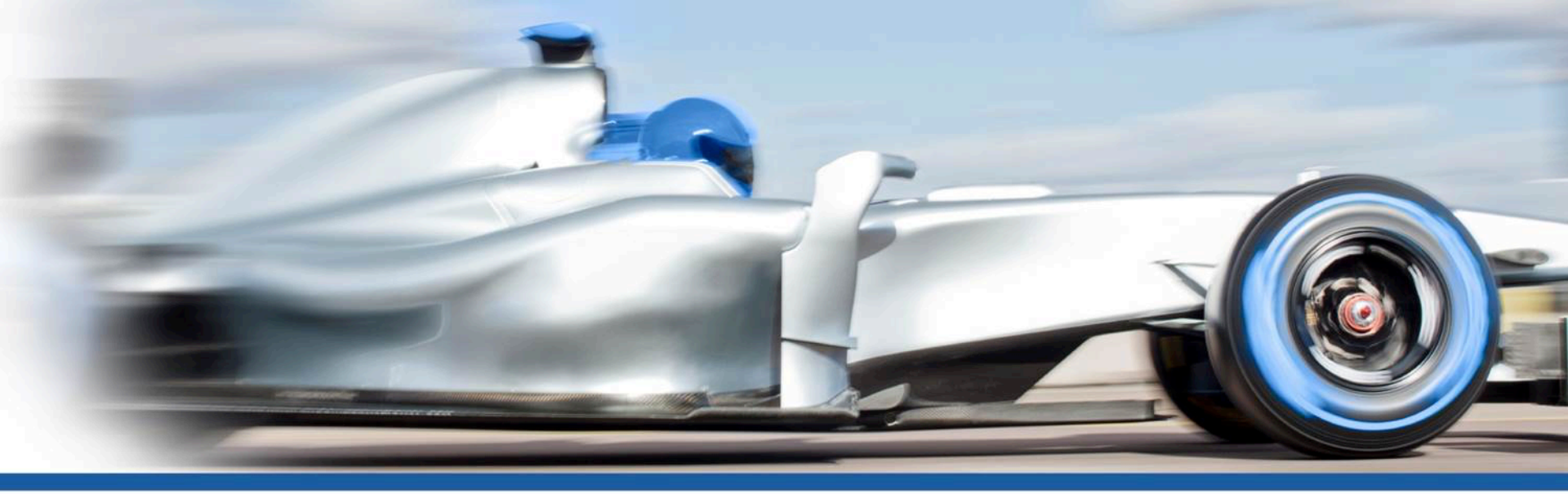
"Drennen installed on his company computer a file-sharing program called "Dropbox," which allows users to transfer information among "linked" devices using an online "cloud" account. Drennen testified that he used the program to aid his work while he was on the road or at home, and linked three personal devices to his Dropbox account while at Free Country: an Android phone, an iPad, and an iMac."

***Free Country Ltd. v. Drennen*, --- F. Supp. 3d ---, 2016 WL 7635516 (S.D.N.Y. 2016).**

The Impact of the Internet of Things

"Sweeping up PII [through the Internet of Things] could violate international or perhaps even domestic data protection laws that proscribe the collection of PII, particularly without the data subject's consent. In addition, transmission or storage methods that lack appropriate security may leave PII vulnerable to hacks or other unauthorized interceptions."

Philip Favro, *IoT Data Collection Raises Legal, eDiscovery Questions*, DATA INFORMED (May 21, 2015).



What best practices should companies follow to better address digital age threats?

GUIDELINES FROM THE NEW IG PLAYBOOK

Navigate with Precision.

DRIVEN

www.driven-inc.com | 1.877.637.4836

Data Mapping

- Essential for an effective incident response after a security breach or cyberattack
- Enables tracking of corporate information to better control ingress and egress of proprietary data
- Advances information retention goals and facilitates better litigation readiness

The New Information Governance Playbook for Addressing Digital Age Threats, **COALITION OF TECHNOLOGY RESOURCES FOR LAWYERS (Sep. 2016).**

Mitigate Damage from Potential Cyberattacks

- Implement an “offensive” email reduction program
- Deploy encryption technologies to protect IP, PII, and other sensitive proprietary materials
- Isolate confidential data “from central data-storage systems connected to the Internet, making it harder to find”
- Use machine learning and automated technologies to facilitate the identification and segregation of proprietary materials

Philip Favro, *The Sony Hack Signals The Need For Information Governance,* INSIDE COUNSEL (Jan. 22, 2015).

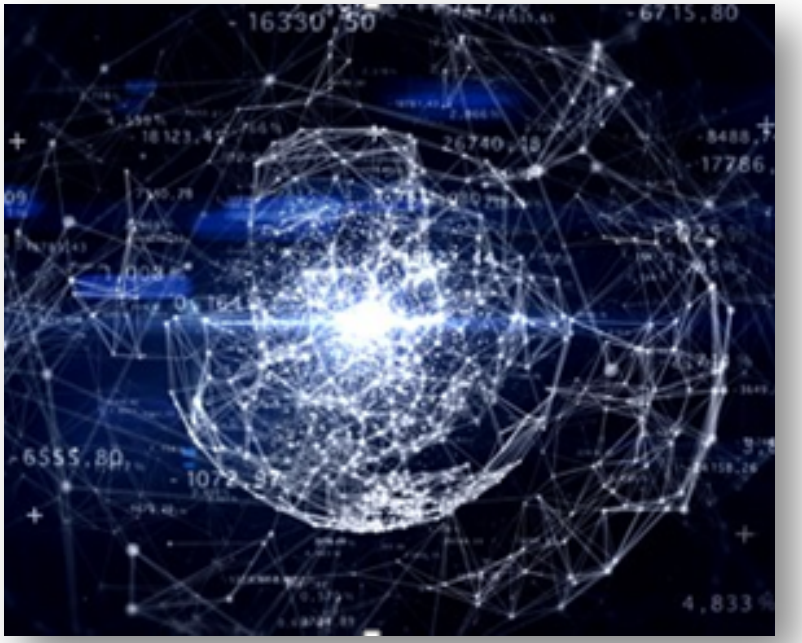
Dealing with Messaging Apps & Other External Sites

- Develop communication and retention guidelines for all collaboration tools
- Limit access to external APIs
- Disable personal drive access and account sharing
- Monitor data uploads and storage
- Enforce auditing of administrative functions
- Limit external party access

Wazid, Mohammad, *Hacktivism trends, digital forensic tools and challenges: A survey,* IEEE Conference on Information & Communication Technologies (ICT) (2013)

Preparing for the Internet of Things

- Create Enterprise CONOPs documentation
- Develop an extended data map
- Determine connectivity and access control features built into enterprise devices
- Develop and train a certified incident response team
- Formalize decommissioning and destruction protocols for IoT devices



Richard Kissel, *Security considerations in the system development life cycle*, NIST SPECIAL PUBLICATION 800-64 (Oct. 2008).

BYODs & BYOCs: Use Policies/Enforcement

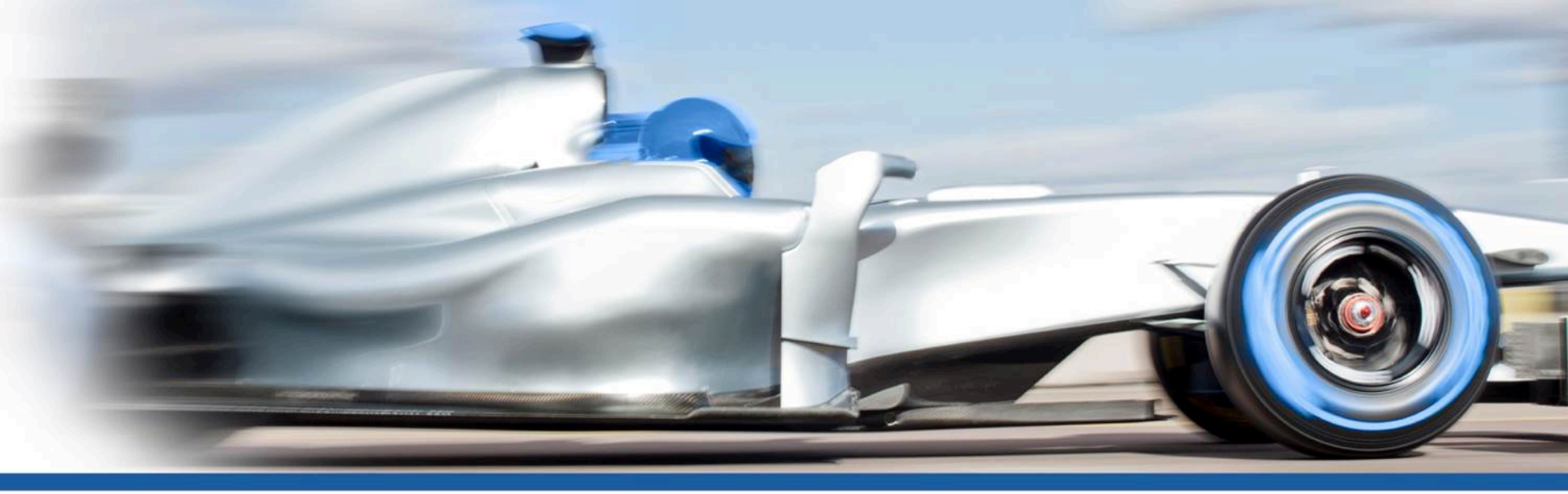
- Educate employees on the nature and extent of applicable policies
- Determine what data can and cannot be accessed or transferred
- Require disclosure of login credentials where applicable and as permitted by law
- Monitor employee use of approved clouds and devices
- Disable devices and accounts upon termination and verify that company data has been destroyed

Philip Favro, *Protecting Corporate Trade Secrets in the Age of Personal Clouds*, THE RECORDER (July 2016).

Banning Devices & Clouds: Use Policies/Enforcement

- Educate employees on the nature and extent of the policy
- Deploy mobile device management solutions and blocking programs
- Monitor employee use of mobile devices and personal clouds
- Discipline for employee noncompliance
- Verification procedures upon employee termination

Philip Favro, *Addressing Employee Use of Personal Clouds*, 22 RICH. J.L. & TECH. 6 (2016)



RESOURCES

Resources

Coalition of Technology Resources for Lawyers

The New Information Governance Playbook for Addressing Digital Age Threats

http://ctrlinitiative.com/wp-content/uploads/2014/07/2016-Guidelines-Regarding-the-Use-of-Technology-Assisted-Review.pdf

Bennett B. Borden & Jason R. Baron

Finding the Signal in the Noise: Information Governance, Analytics, and the Future of Legal Practice

20 RICH. J.L. & TECH. 7 (2014)

Resources

Jason R. Baron & Amy Ramsey Marcos

Beyond BYOD: What Lies in the Shadows

ETHICAL BOARDROOM, Aug. 10, 2015

Philip J. Favro

The Sony Hack Signals the Need for Information Governance

INSIDE COUNSEL (Jan. 22, 2015)

BUSINESS INSIGHTS FOR THE LEGAL PROFESSIONAL

Q & A