



# Welcome to the Cyber Risk Insights Conference!



# Welcoming Remarks



**Rebecca Bole**  
EVP & Editor-in-Chief  
Advisen





Leading the way to smarter and more  
efficient risk and insurance communities,  
Advisen delivers:

- The **right** information into
- The **right** hands at
- The **right** time
- To power *performance*

# Thank you to our Advisory Board

Steve Anderson, QBE [2017 Conference Co-Chair]

Emy R. Donovan, Allianz

Tim Francis, Travelers

Leslie Kesselring, Kesselring Communications

Garrett Koehn, CRC Insurance Group

Pascal Millaire, Symantec [2017 Conference Co-Chair]

Michael Palotay, NAS Insurance

Lisa Phillips, Wells Fargo Insurance



# Thanks to our Sponsors!

**NAS** insurance



**TRAVELERS** 



**ThreatMetrix**®  
The Digital Identity Company™

 **WILSON ELSER**  
WILSON ELSE MOSKOWITZ EDELMAN & DICKER LLP



crowell  moring



**BITSIGHT**®  
The Standard in SECURITY RATINGS







**Rise.  
Read FPN.  
Shine.**

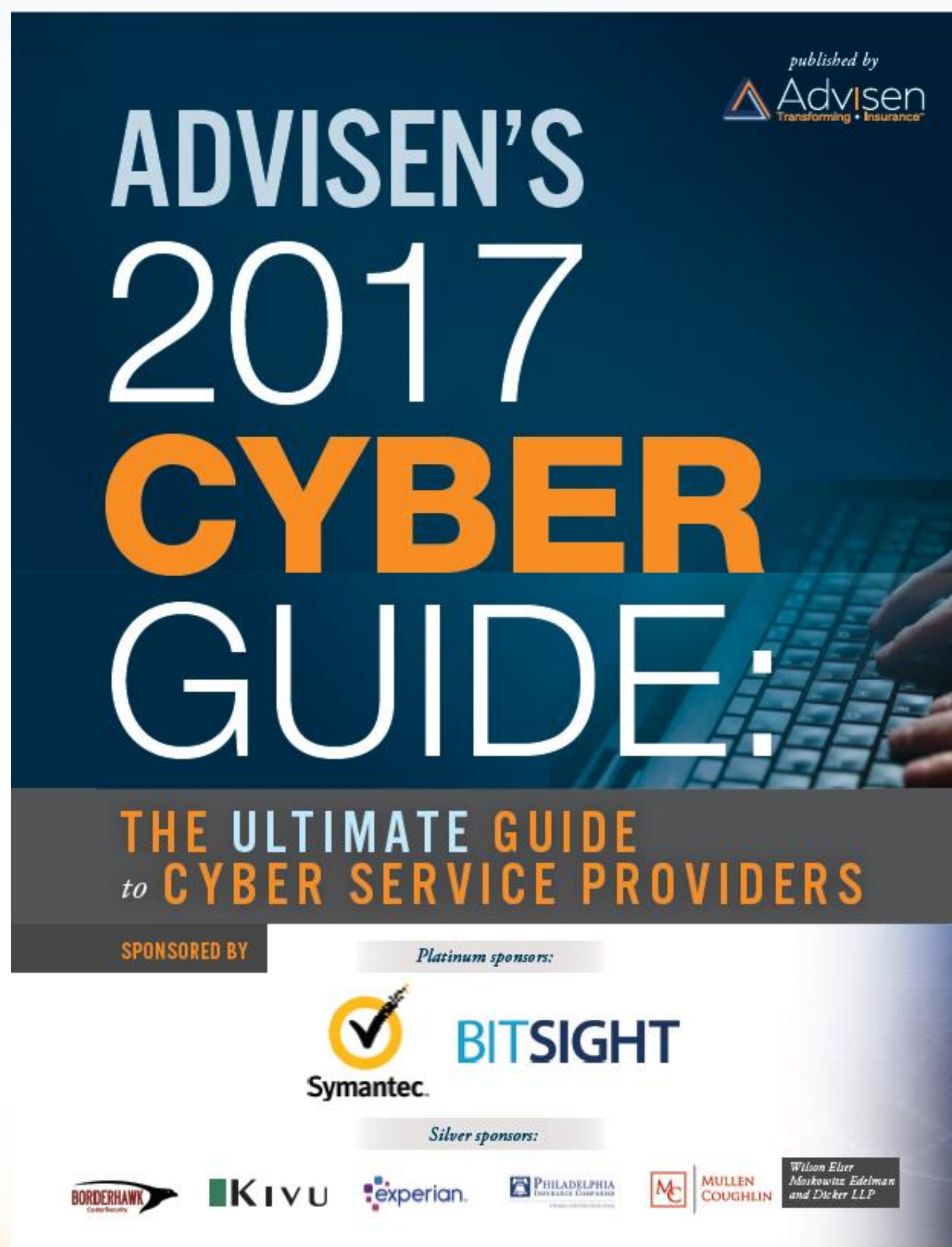
Make the industry's top  
stories a part of your daily  
morning routine.



Sign up for your free FPN Professional trial at:  
<http://info.advisenltd.com/fpn-30-day-trial/>



# Coming soon!



*Sponsored by:*

**Symantec, Bitsight  
Borderhawk, Kivu Consulting,  
Experian, Philadelphia  
Insurance Companies,  
Mullen Coughlin, Wilson Elser**



# SYMANTEC

WWW.SYMANTEC.COM



Public or private: PUBLIC

Annual revenue: >\$250M TO \$500M

Number of Employees: >1000

CEO: GREG CLARK

Year Founded: 1982

Geographic reach: GLOBAL

Number of Clients: 370,000



Symantec

## ABOUT SYMANTEC:

Symantec Cyber Insurance provides a robust cyber security analytics platform for underwriters, p and actuaries to measure cyber risk, leveraging the power of Symantec's cyber security intelligence cyber security with a diverse product portfolio, we provide unique partnership solutions to impro policyholders against emerging cyber threats. Symantec helps the world's leading insurers better u themselves and for their clients.

Key areas:

- Underwriting intelligence
- Cyber risk modeling
- Pricing analytics
- Security product partnerships

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest c threats, and protect more customers from the next generation of attacks. We help companies, gov most important data wherever it lives.



Pascal Millaire,  
VP & GM, Cyber Insurance

- Does your company integrate third-party data

350 Ellis Street • Mountain View, CA 94043  
408-314-4415  
Sudhir Bharti  
cyber\_insurance@symantec.com

## BITSIGHT TECHNOLOGIES

WWW.BITSIGHTTECH.COM



Public or private: PRIVATE

Annual revenue: >\$25M TO \$100M

Number of Employees: >100 TO 250

CEO: SHAUN MCCONNON

Year Founded: 2011

Geographic reach: GLOBAL

Number of Clients: 500+

Client Industry focus: ALL

**BITSIGHT**  
The Standard in SECURITY RATINGS

## ABOUT BITSIGHT TECHNOLOGIES:

As the Standard in Security Ratings, the BitSight Technologies mission is to significantly help reduce risk for all organizations. BitSight invented the concept of security risk ratings for companies using publicly accessible data. BitSight is the only company who has independently verified studies that correlate our ratings system to data breaches. BitSight's data provides risk ratings and the underlying data for those engaged in vendor/third party risk management (VRM), self risk assessment (benchmarking), vendor selection, mergers and acquisitions, and for cyber-insurance underwriting. BitSight allows our customers to have a combination of both continuous monitoring along with periodic reporting so they have the latest and most accurate information available. Much of the monitoring can be done via automated alerts but regular interaction with the BitSight platform will provide insights that will greatly enhance security and risk process, assessments, and daily operations.

BitSight transforms how companies manage security risk. Our software-as-a-service (SaaS) offering objectively rates a company's security effectiveness by analyzing data observable from outside a company's network. Unlike the manual and subjective assessments used to manage risk today, BitSight's automated service provides daily ratings based on verifiable and actionable evidence. Our sophisticated analytics and alerting capabilities provide risk managers the insight they need to proactively identify, quantify, and mitigate the risk of being exposed to a breach.



Shaun McConnon, CEO

- How many products or applications does your company offer?  
We have two main products. The first is BitSight Security Ratings, which supports Cyber Insurance, Vendor Risk Management, Benchmarking, and Mergers and Acquisitions use cases. The second is Discover which supports Enterprises with vendor discovery and Cyber Insurers with better insights on risk aggregation.
- What is your company's secondary business focus?  
Insurance data & analytics (risk assessment and quantification)
- How many insurance carriers does your company partner with? 10
- Does your company integrate third-party data with your solutions?  
Yes, along with our own proprietary data sources including anubisnetworks, we work with a number of different data partners, but have confidentiality agreements in place. We are contractually obligated not to reveal the names of our partners.

125 CambridgePark Drive, Suite 204 • Cambridge, MA 02140  
617-245-0469  
Liz Robinson  
liz.robinson@bitsighttech.com

**Adv|sen**  
Transforming • Insurance™

“The most comprehensive, single source of cyber service providers to date”

**Adv|sen**  
Transforming • Insurance™





  
**Cyber Risk  
Awards**  
2017

**JUNE 14, 2017 • NEW YORK, NY**

Submit your nominations today!

[www.advisenltd.com/media/awards/06/14/2017-cyber-risk-awards](http://www.advisenltd.com/media/awards/06/14/2017-cyber-risk-awards)

## THE 2017 AWARD CATEGORIES:

CYBER RISK INDUSTRY PERSON OF THE YEAR- USA,  
LONDON AND INTERNATIONAL MARKETS

CYBER RISK EVENT RESPONSE TEAM OF THE YEAR

CYBER RISK PRE-BREACH TEAM OF THE YEAR

CYBER RISK INNOVATION OF THE YEAR

CYBER SERVICE VENDOR OF THE YEAR

CYBER NEWCOMER OF THE YEAR - **NEW**

CYBER LAW FIRM OF THE YEAR - **NEW**

CYBER REINSURER OF THE YEAR - **NEW**

CYBER RISK BROKING TEAM OF THE YEAR

CYBER RISK INSURER OF THE YEAR



# Co-Chair Opening Remarks



**Steve Anderson**

Vice President, Product Executive –  
Privacy & Network Security  
Specialty Insurance  
QBE



**Pascal Millaire**

VP & GM  
Symantec



# What's new on the agenda for the Advisen SF CRIC in 2017?





# What's new on the agenda for the Advisen SF CRIC in 2017?

Cyber insurance is a dynamic market and this year's conference reflects the changing marketplace over the past 12 months

- **Theme One:** Internet of Things Becomes Moves from Theory to Reality for Insurers
- **Theme Two:** There's Increasingly More To Cyber Insurance Than **Data Breaches**
- **Theme Three:** Cyber Insurance **Modeling** *Begins* To Come Of Age
- **Theme Four:** As The Cyber Insurance Industry Grows, New **Growing Pains** Emerge With Its Size
- **Theme Five:** **Government** Becomes A More Important Constituent For Cyber Insurers





# The Internet of Threats: The New Paradigm



# The Internet of Threats: The New Paradigm



**Dean Coclin**  
Sr. Director of Business  
Development, Website Security  
Symantec

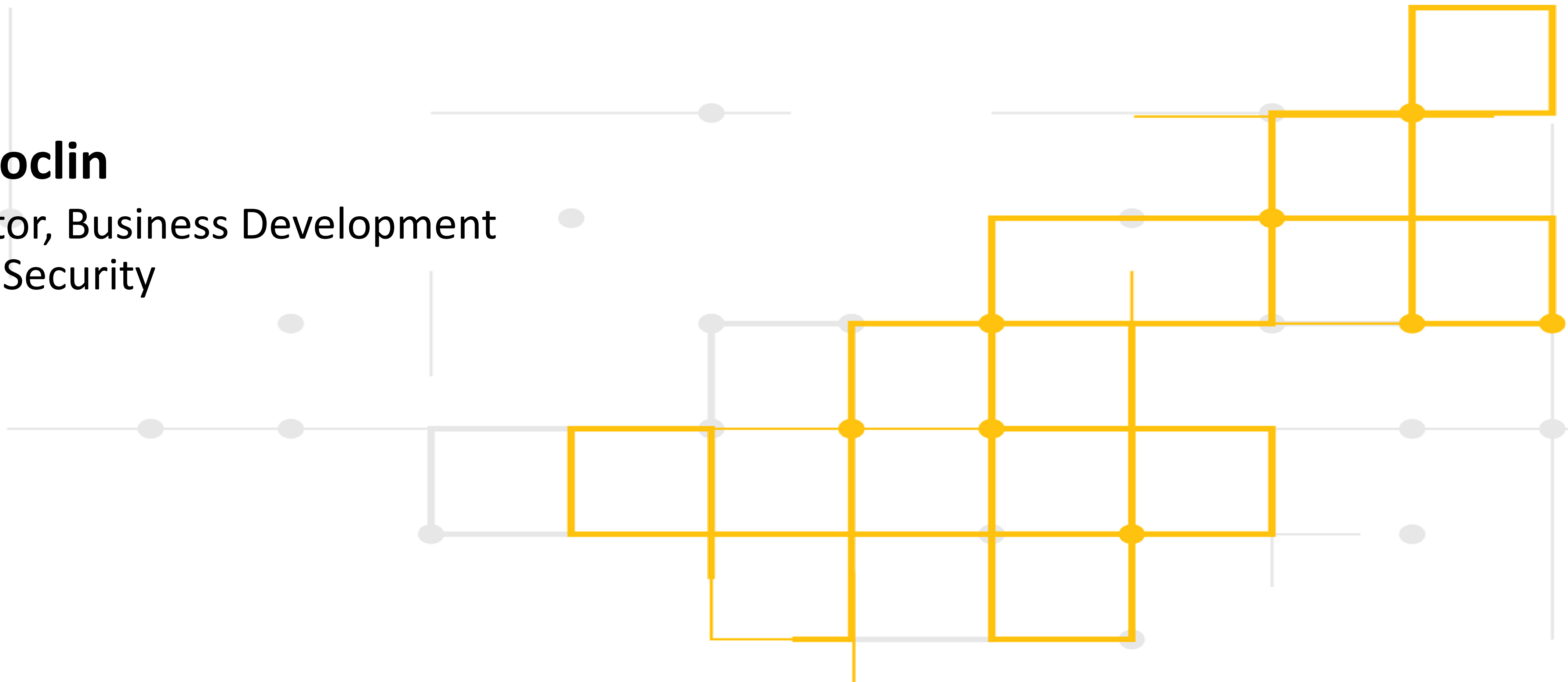




# The Internet of Threats: The New Paradigm

**Dean Coclin**

Sr. Director, Business Development  
Website Security







Trying to determine the market size of the Internet of Things is like trying to calculate the market for plastics, circa 1940. At that time, it was difficult to imagine that plastics could be in everything. If you look at information processing in the same way, you begin to see the vast range of objects into which logic, processors, or actuators could be embedded.



- Michael Nelson,  
Bloomberg Government &  
Georgetown University





Trying to determine the market size of the *Internet of Things (IoT)* is like trying to calculate the market for **the internet, circa 1994**. At that time, it was difficult to imagine that **the internet** could be in everything. If you look at information processing in the same way, you begin to see the vast range of objects into which logic, processors, or actuators could be embedded.



- Michael Nelson,  
Bloomberg Government &  
Georgetown University



# What is Internet of Things?

- The **Internet of Things (or IoT)** is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.







**Which are these “things”?**

Let's take a look...





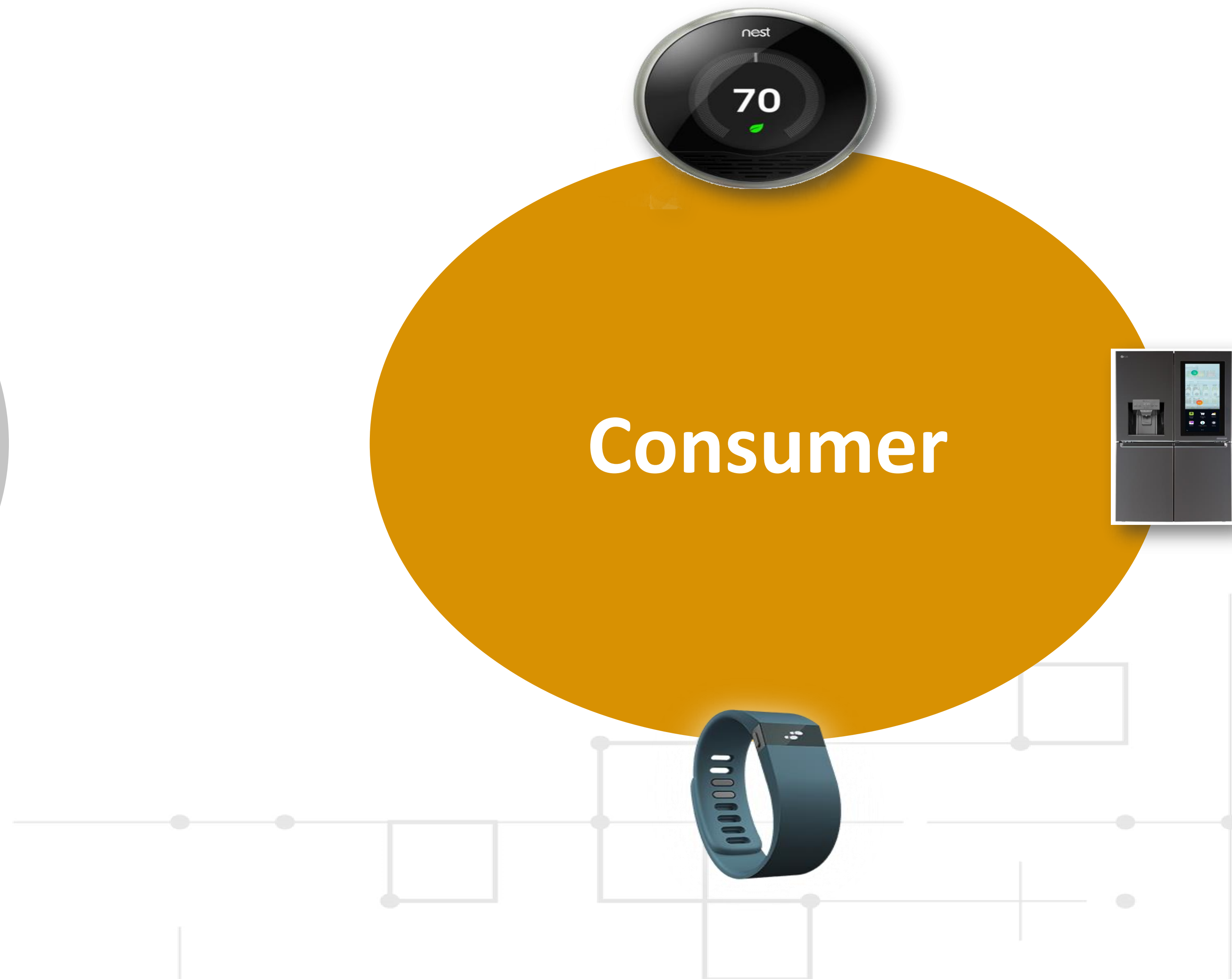
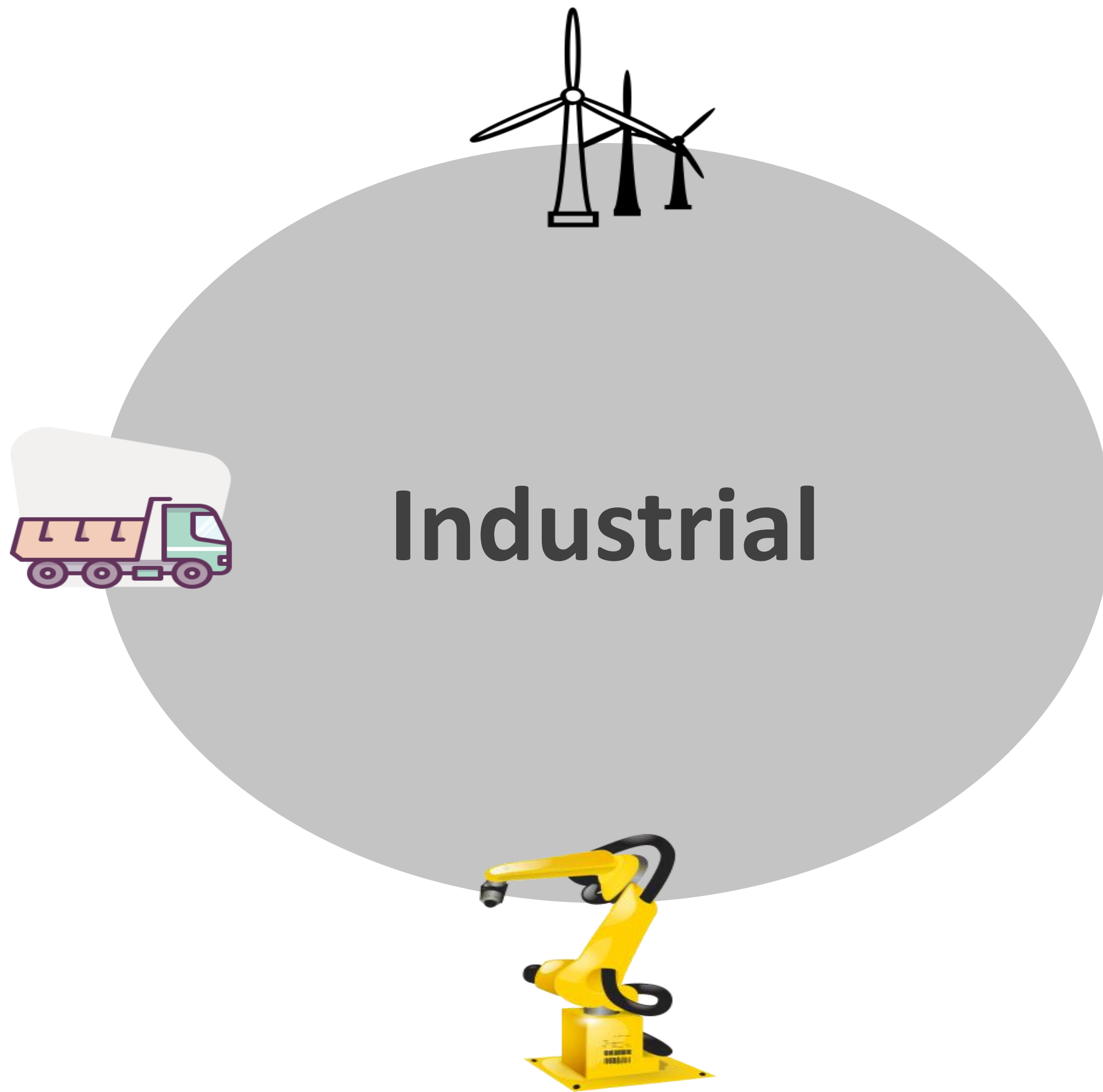


# Internet of Things - Types

- **Industrial IoT:** Application of Internet of Things (IoT) technologies in manufacturing
- **Consumer IoT:** Related to connected devices aimed at the consumer market.
- **Machine to Machine IoT:** Machine to Machine IoT is a subset of Industrial IoT that focuses on machine to machine communication



# Internet of Things - Types





**What could go wrong?**



## Technology

### Fiat Chrysler recalls 1.4 million cars after Jeep hack

24 July 2015 | Technology



Fiat Chrysler has issued a safety recall affecting 1.4m vehicles in the US, after security researchers showed that one of its cars could be hacked.

On Tuesday, tech magazine Wired reported that hackers had taken control of a Jeep Cherokee via its internet-connected entertainment system.

Hackers took  
control of a  
**Jeep Cherokee**  
via IoT



“Once external security is *breached*, hackers can have free rein to access onboard vehicle computer systems which manage everything from engines and brakes to air conditioning.”



The image is a screenshot of a Reuters news article. At the top, the Reuters logo is visible on the left, and 'EDITION: U.S.' is on the right. Below the logo is a navigation bar with links: HOME, BUSINESS, MARKETS, WORLD, POLITICS, TECH, OPINION, and BREAKINGVIEWS. A large orange banner with the text 'VOTE FOR US' is positioned below the navigation bar. To the right of this banner, there is a section for 'Inside Market Data Awards' and 'Inside Reference Data Awards' with a 'Vote Now >' button. The main headline of the article is 'BMW fixes security flaw in its in-car software'. Below the headline, it says 'FRANKFURT | Fri Jan 30, 2015 10:15am EST'. There are social media sharing buttons for Twitter (180), LinkedIn (100), Facebook, and Email, along with a 'Print' button. The article text begins with 'Jan 30 (Reuters) - German luxury carmaker BMW has fixed a security flaw that could have allowed hackers to unlock the doors of up to 2.2 million Rolls-Royce, Mini and BMW vehicles, it said on Friday.' It continues with 'BMW said officials at German motorist association ADAC had identified the problem, which affected cars equipped with the company's ConnectedDrive software using on-board SIM cards -- the chips used to identify authorised users of mobile devices.' The next paragraph states 'BMW drivers can use the software and SIM cards to activate door locking mechanisms, as well as a range of other services including real-time traffic information, online entertainment and air conditioning.' The following paragraph says 'The security risk occurred when data was transmitted, BMW said, adding it did not impede the car's critical functions of driving, steering or braking.' The final paragraph in the image says 'BMW said it was not aware of any examples where the data had been used to compromise the security of a vehicle.'

REUTERS

EDITION: U.S.

SIGN IN

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

VOTE FOR US

Inside Market Data Awards  
Inside Reference Data Awards  
Vote Now >

## BMW fixes security flaw in its in-car software

FRANKFURT | Fri Jan 30, 2015 10:15am EST

Tweet 180 in Share 100 f Share this 8+1 56 Email Print

### RELATED NEWS

REFILE-UPDATE 2- Facebook takes blame for service outages, which hit wider Web

### ANALYSIS & OPINION

Review: The Mad Men are watching you

What was behind Israel's strike in Syria that killed an Iranian general?

Jan 30 (Reuters) - German luxury carmaker BMW has fixed a security flaw that could have allowed hackers to unlock the doors of up to 2.2 million Rolls-Royce, Mini and BMW vehicles, it said on Friday.

BMW said officials at German motorist association ADAC had identified the problem, which affected cars equipped with the company's ConnectedDrive software using on-board SIM cards -- the chips used to identify authorised users of mobile devices.

BMW drivers can use the software and SIM cards to activate door locking mechanisms, as well as a range of other services including real-time traffic information, online entertainment and air conditioning.

The security risk occurred when data was transmitted, BMW said, adding it did not impede the car's critical functions of driving, steering or braking.

BMW said it was not aware of any examples where the data had been used to compromise the security of a vehicle.

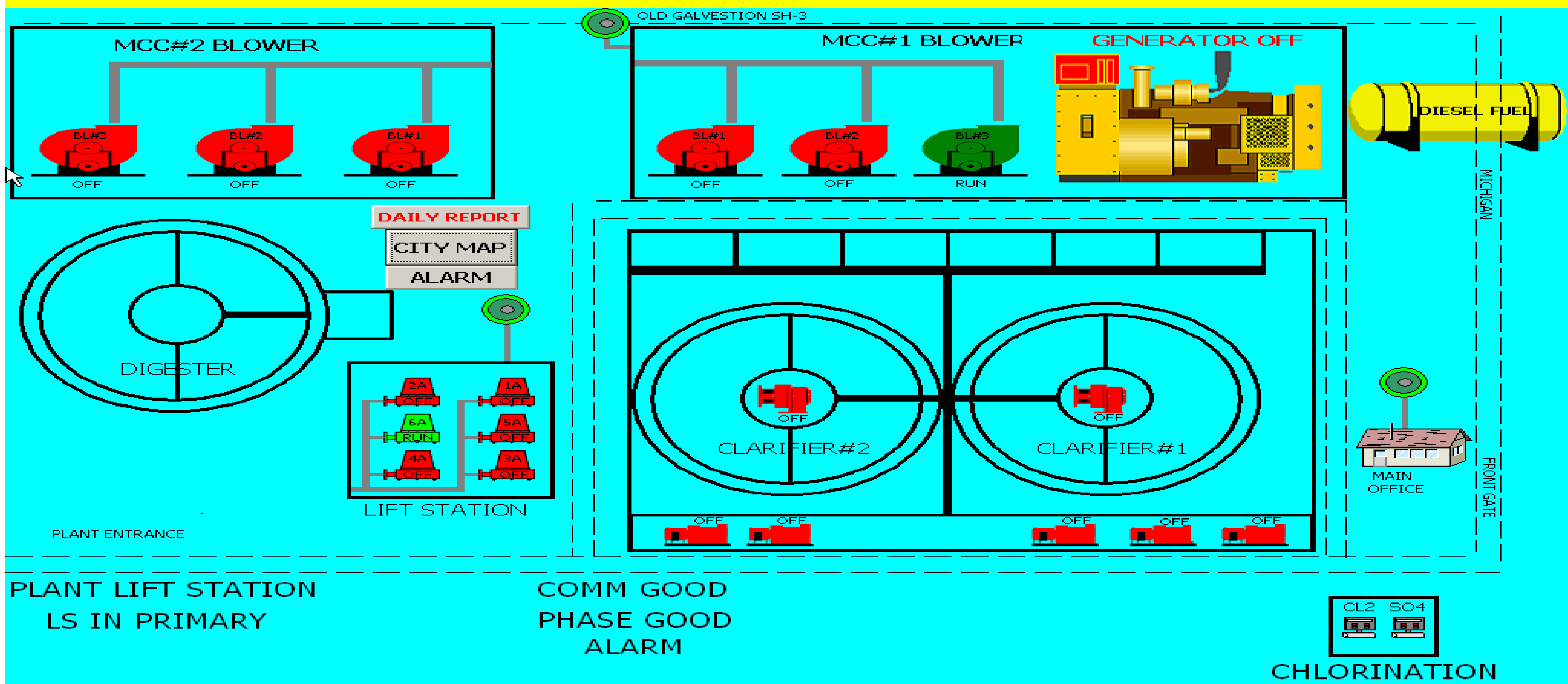






# Hacker Says Texas Town Used **Three Character Password** To Secure Internet Facing SCADA System

## CITY OF SOUTH HOUSTON WASTE WATER TREATMENT PLANT





“

This was barely a hack. A child who knows how the HMI that comes with Simatic works could have accomplished this. I'm sorry this ain't a tale of advanced persistent threats and stuff, but frankly most compromises I've seen have been a result of gross stupidity, not incredible technical skill on the part of the attacker. Sorry to disappoint.”

”

***“Pr0f” in an e-mail interview with Threat Post.***



“

We're probably not the only one who is wide open.  
He caught everyone with our pants down.

”

*South Houston Mayor Joe Soto*



mozilla

[Click here](#) if you believe the Web should be a force for good.  Firefox

THREAT LEVEL

## It's Insanely Easy to Hack Hospital Equipment

### It's Insanely Easy to Hack Hospital Equipment

“Everything was tested, and most of it was hackable.”

“drug infusion pumps . . . that can be remotely manipulated

“temperature settings on refrigerators storing blood and drugs that can be reset

“X-rays that can be accessed by outsiders”

Photo: Charles Thatcher/Getty Images



mozilla

[Click here](#) if you believe the Web should be a force for good.  Firefox

THREAT LEVEL |

## It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | [PERMALINK](#)

**“weak passwords . . . default and hardcoded vendor passwords like ‘admin’ or ‘1234’; and embedded web servers and administrative interfaces that make it easy to identify and manipulate devices”**



Photo: Charles Thatcher/Getty Images



mozilla

[Click here](#) if you believe the Web should be a force for good.  Firefox

THREAT LEVEL |

## It's Insanely Easy to Hack Hospital Equipment

BY KIM ZETTER 04.25.14 | 6:30 AM | [PERMALINK](#)

**“there was one bright spot . . . anesthesia equipment and ventilators are generally not networked and don’t allow web administration”**



Photo: Charles Thatcher/Getty Images



# Internet of Things – Attack Types

- **Demand Ransom:** Make valuable data unusable unless a ransom is paid
- **Steal Information:** Steal personal or private information and sell it on the Dark Web
- **Access Remote Devices:** Access remotely controlled devices such as security cameras or baby monitors



# Internet of Things – Intruder Types

- **Individuals:** Individual hackers who work alone and use social engineering to target systems
- **Organized Groups:** Target specific organizations for revenge or theft of trade secrets
- **Intelligence Agencies:** Probe the military systems of other countries for specific purposes

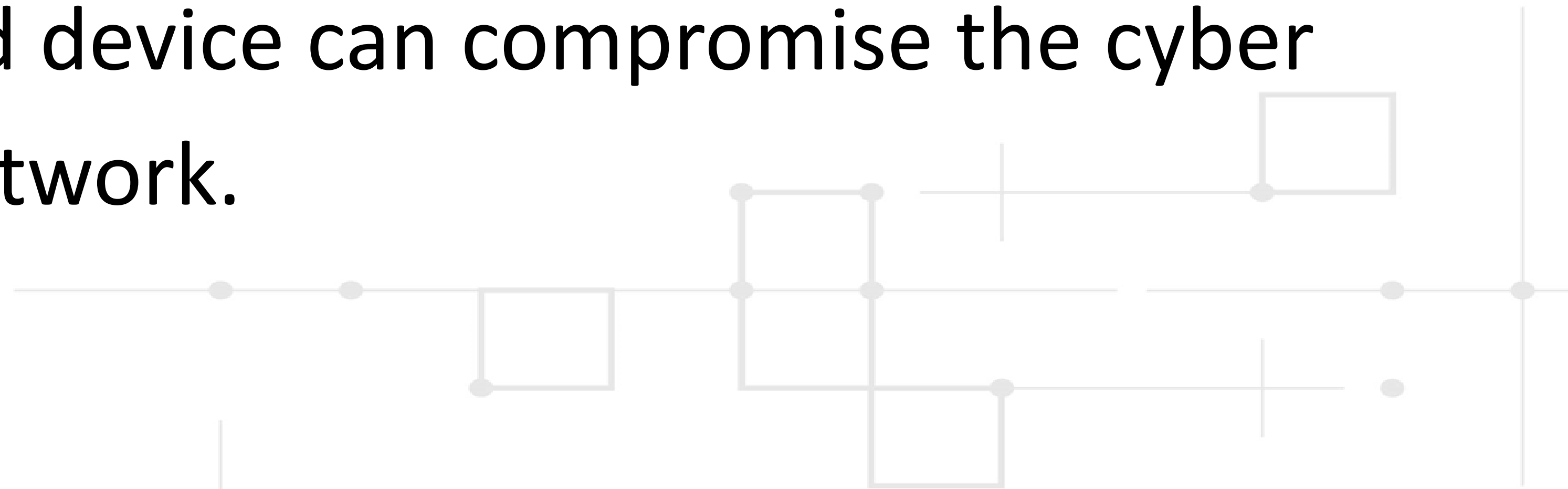


# What are the risks to businesses and consumers?



# Internet of Things – Business & Consumer Risk

- **Personal Information:** Businesses, using IoT devices, need to understand what personal information is being collected, how it is being used and who has access to it.
- **Single Point of Failure:** A single point of vulnerability in a networked or connected device can compromise the cyber security of the entire network.





# Mirai and the DDoS Attack on Dyn

- **How does Mirai Work:** Continuously scans for IoT devices protected by factory default credentials. Mirai infects devices with malware by turning them into a bot that can be used in DDoS attacks.
- **Devices at Risk:** Routers, DVRs, CCTV cameras, and any other 'smart', internet-connected appliances are at risk of such attacks.



# What role can government or regulators play in IoT?

# Internet of Things – Government's Role

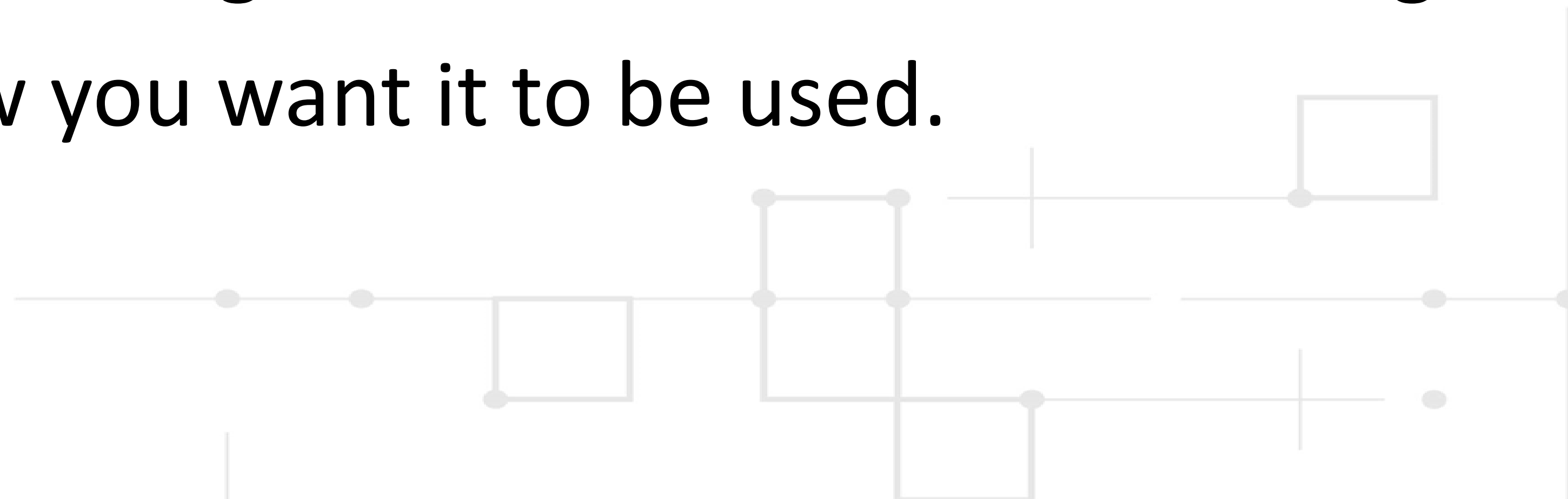
- **NIST Framework:** Enable manufacturers to adopt security standards and build products with user safety in mind.
- **Focus on Security Upgrades:** Help consumers understand security upgrades for the Internet of Things products.



**Can we be safe?**

# Things to Consider

- “Should it be connected” – NOT “can it be connected.”
- Security in the IoT is a **necessity** and **enabler**, not a burden or a tax.
- Assume people will do wrong – think about how something could be used, not how you want it to be used.





# IoT Cyber Security Alliance

- **Purpose:** Leverage combined expertise to allay business concerns about the Internet of Things and solve its security challenges
- **Immediate Steps:** Conduct collaborative research and raise awareness on IoT security challenges across verticals such as health care, automotive, and industrial.



# Q & A





# Thank you!

## Dean Coclin

Sr. Director, Business Development

Website Security

@chosensecurity

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit [www.symantec.com](http://www.symantec.com) or connect with us on Facebook, Twitter, and LinkedIn.

Copyright © 2016 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.

# IoT: Weighing up the ‘Possible’ against the ‘Value’



# IoT: Weighing up the 'Possible' against the 'Value'



**Steve Anderson**

VP, Product Executive –Privacy &  
Network Security Specialty Insurance

QBE

Moderator



# IoT: Weighing up the 'Possible' against the 'Value'

- **Steve Anderson**, VP, Product Executive – Privacy & Network Security Specialty Insurance, QBE (Moderator)
- **Elisabeth Case**, Senior Vice President, Cyber Advisory Practice Leader, Marsh
- **Alisdair Faulkner**, Co-Founder, Chief Products Officer, ThreatMetrix
- **Kevin Kirst**, Director, Cyber Crime and Breach Response, PwC



# IoT: Weighing up the 'Possible' against the 'Value'



**Steve Anderson**  
QBE



**Elisabeth Case**  
Marsh



**Alisdair Faulkner**  
ThreatMetrix



**Kevin Kirst**  
PwC





# The Regulatory View on IoT



# The Regulatory View on IoT



**Emy R. Donovan**  
Head of Cyber, North America  
Allianz  
Moderator



# The Regulatory View on IoT

- **Emy R. Donovan**, Head of Cyber, North America, Allianz (Moderator)
- **Adam Hamm**, Managing Director, Protiviti Global Consulting
- **Ellen MacDonald Farrell**, Senior Counsel Washington, D.C., Crowell & Moring
- **Wes McClelland**, Vice President, Federal Affairs, American Insurance Association



# The Regulatory View on IoT



**Emy R. Donovan**  
**Allianz**



**Adam Hamm**  
**Protiviti Global Consulting**



**Ellen MacDonald Farrell**  
**Crowell & Moring**



**Wes McClelland**  
**American Insurance  
Association**





# Afternoon Break

**Coming up next...**  
Business Interruption



# Thanks to our Sponsors!

**NAS** insurance



**TRAVELERS** 



**ThreatMetrix**  
The Digital Identity Company



crowell  moring



**BITSIGHT**  
The Standard in SECURITY RATINGS







# Business Interruption



# Business Interruption



**Thomas Reagan**  
Managing Director  
Marsh  
Moderator





# Business Interruption

- **Thomas Reagan**, Managing Director, Marsh (Moderator)
- **Christopher M. Calnon**, Senior Vice President, Financial Lines, Chubb
- **Richard Sunny**, Operations Vice President, Operations Claims Manager, FM Global



# Business Interruption



**Thomas Reagan  
Marsh**



**Christopher M. Calnon  
Chubb**



**Richard Sunny  
FM Global**



# A Study on Insurance Risk Aggregation



# A Study on Insurance Risk Aggregation



**Mickey Estey**  
Senior Vice President,  
E&O/Cyber/Media,  
RT ProExec – RT Specialty  
Moderator





# A Study on Insurance Risk Aggregation

- **Mickey Estey**, Senior Vice President, E&O/Cyber/Media, RT ProExec – RT Specialty (Moderator)
- **Brad Gow**, Senior Vice President, Endurance
- **John E. Howell**, Partner, Wiley Rein LLP
- **Kara Owens**, Vice President, TransRe





## **IOT exposure creates potential for liability and loss** **because of:**

- **Interconnectedness** - devices/things are connected
- **Large Numbers** - the volume of connected devices/things
- **What is connected** - the different types of connected devices/things

## Silent Cyber Defined

- Unknown amounts and types of coverage provided for a given loss based on an absence of exclusions



## IOT losses to Cyber policies

- Privacy exposures – PII, online behavioral data, voice (Alexa/Echo)
- DDoS attacks – Dyn attack (near miss)
- Ransomware of things (car, refrigerator, HVAC, medical device, cameras, TV's)
- Business Interruption



## **IOT losses to Property/GL/Other (3<sup>rd</sup>/1<sup>st</sup> Party)**

### **What other policies can be impacted?**

- Marine, Aviation, Product Recall, Auto, Energy
- Bodily Injury (medical devices, healthcare)
- Personal and Advertising injury (publication that violates a right to privacy; wrongful entry; invasion of right to private occupancy.)
- Property Damage (HVAC, manufacturing, utilities)
- Business Interruption - DDoS attacks, hacking, system failure
- E&O (tech, healthcare, miscellaneous)
- D&O (shareholder lawsuits; regulator claims)



## **IOT – Armageddon Scenario 1** **Traffic Control Failure**

- **Attack on smart grid (impacting M2M communication)**
- **Causation: Terrorism related**
- **Potential Losses: business interruption, physical damage, bodily injury**
- **Policies triggered: Property, Cyber, GL, etc.**
- **Aggregation: Across various insurance product lines**

## IOT – Armageddon Scenario 2 Service Provider Failure

- Coordinated DDoS attack on a common service provider(s)
- Causation: Mirai botnet
- Potential Losses: Widespread business interruption
- Policies triggered: Cyber policy
- Aggregation: Multiple policies triggered in cyber portfolio



## **IOT – Armageddon Scenario 3** **Medical Device Failure**

- **Attack on medical devices**
- **Causation: Targeted Malware Implanted by Bad Actor**
- **Potential Losses: privacy breach, bodily injury**
- **Policies triggered: PHs could include manufacturers, med sales reps, hospitals, testing lab, software vendors and consultants, retailers; policies may include product liability, E&O, cyber, recall, GL, etc.**
- **Aggregation: Multiple policies potentially triggered in cyber portfolio and various insurance product lines**

## **IOT – How do insurance companies identify, monitor and aggregate these exposures?**

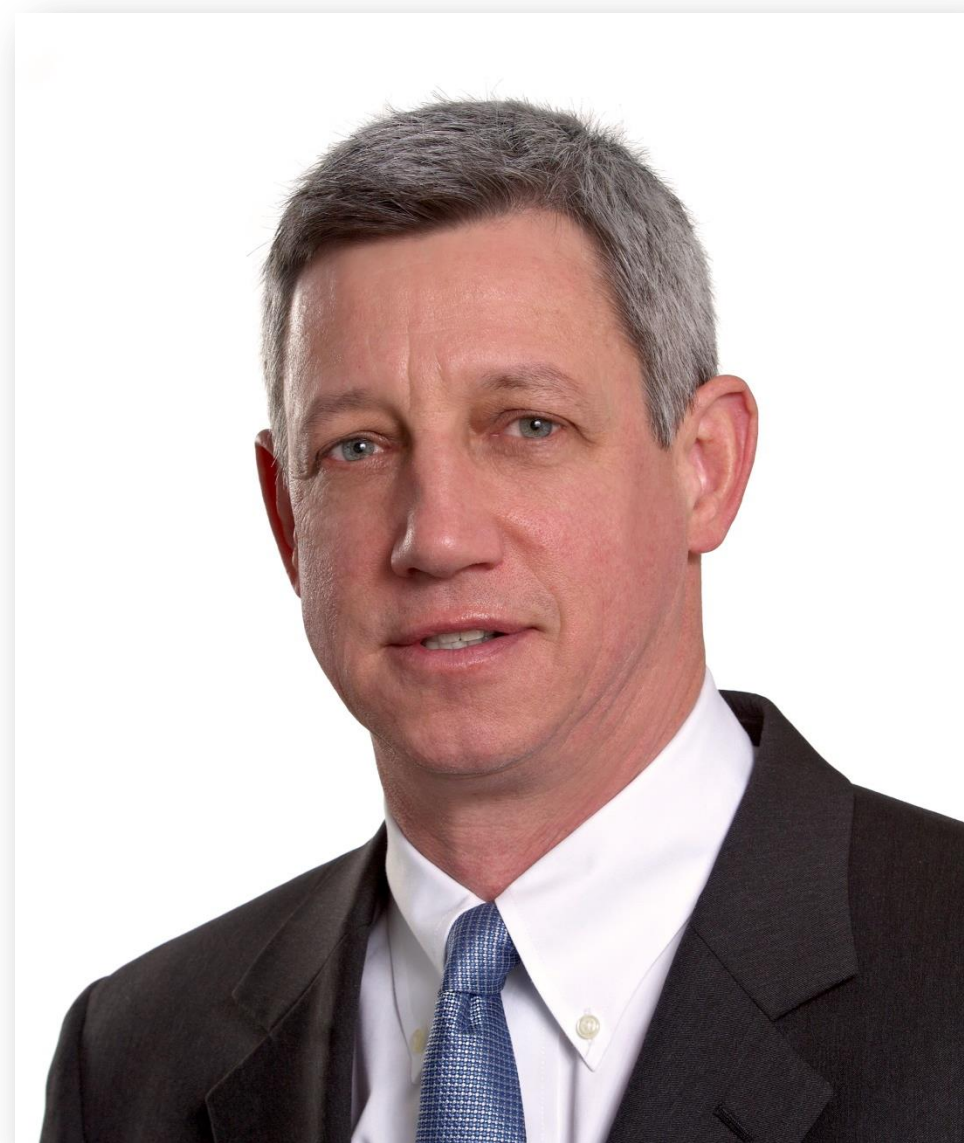
- **Tracking exposures – how is it done? What does ‘limited exposure’ actually mean?**
- **Introduction of Lloyd’s Cyber Framework– discuss, similar US adoption?**
- **Clash vs aggregation - How do you look at each?**
- **What does the future hold?**



# A Study on Insurance Risk Aggregation



**Mickey Estey**  
RT ProExec-RT Specialty



**Brad Gow**  
Endurance



**John E. Howell**  
Wiley Rein LLP



**Kara Owens**  
TransRe



# Closing Remarks & Reception Sponsored by:



**Symantec™**



# Thanks to our Sponsors!

**NAS** insurance



**TRAVELERS** 



**ThreatMetrix**®  
The Digital Identity Company™

 **WILSON ELSE**  
WILSON ELSE MOSKOWITZ EDELMAN & DICKER LLP



crowell  moring



**BITSIGHT**®  
The Standard in SECURITY RATINGS

