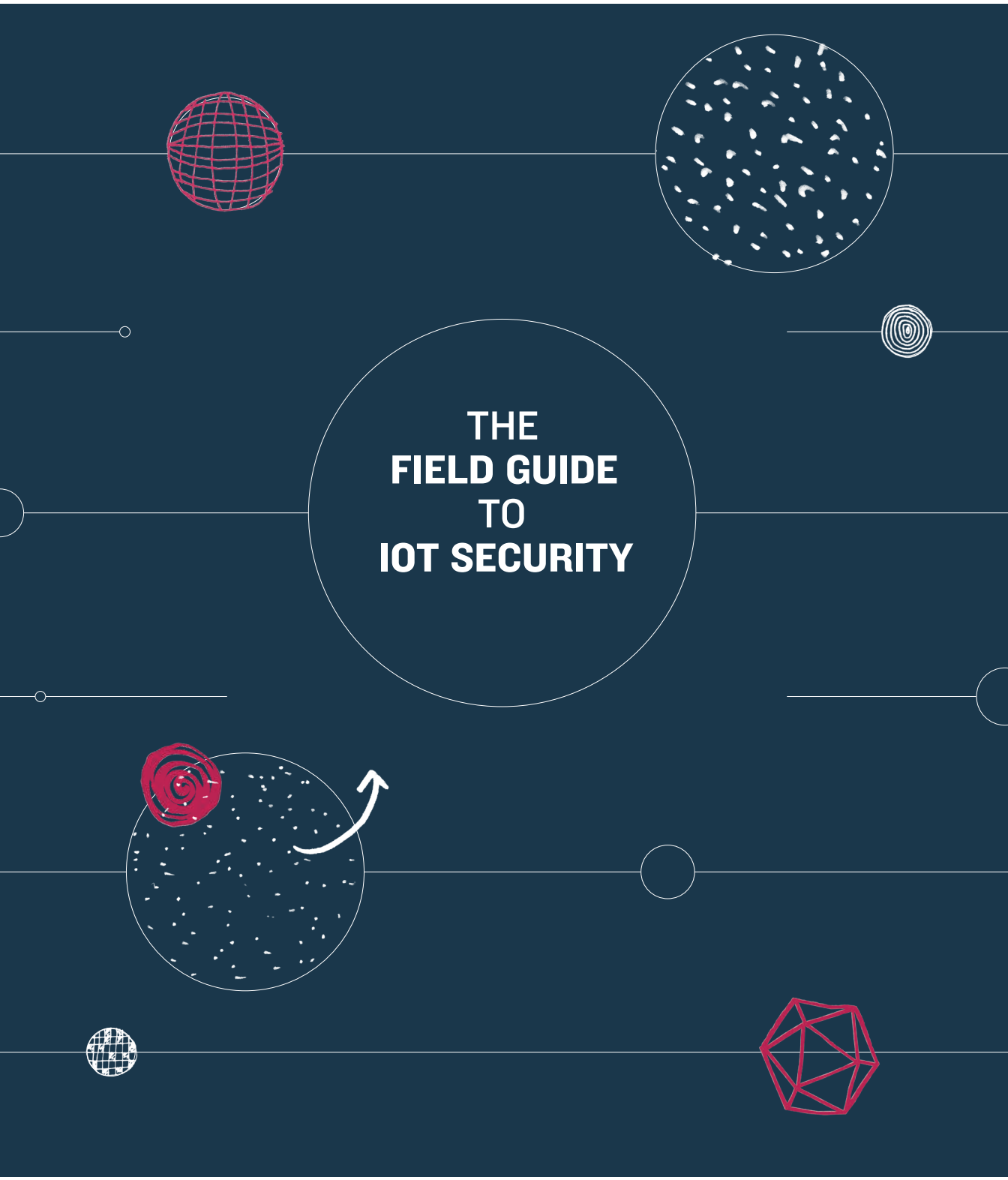
Booz | Allen | Hamilton



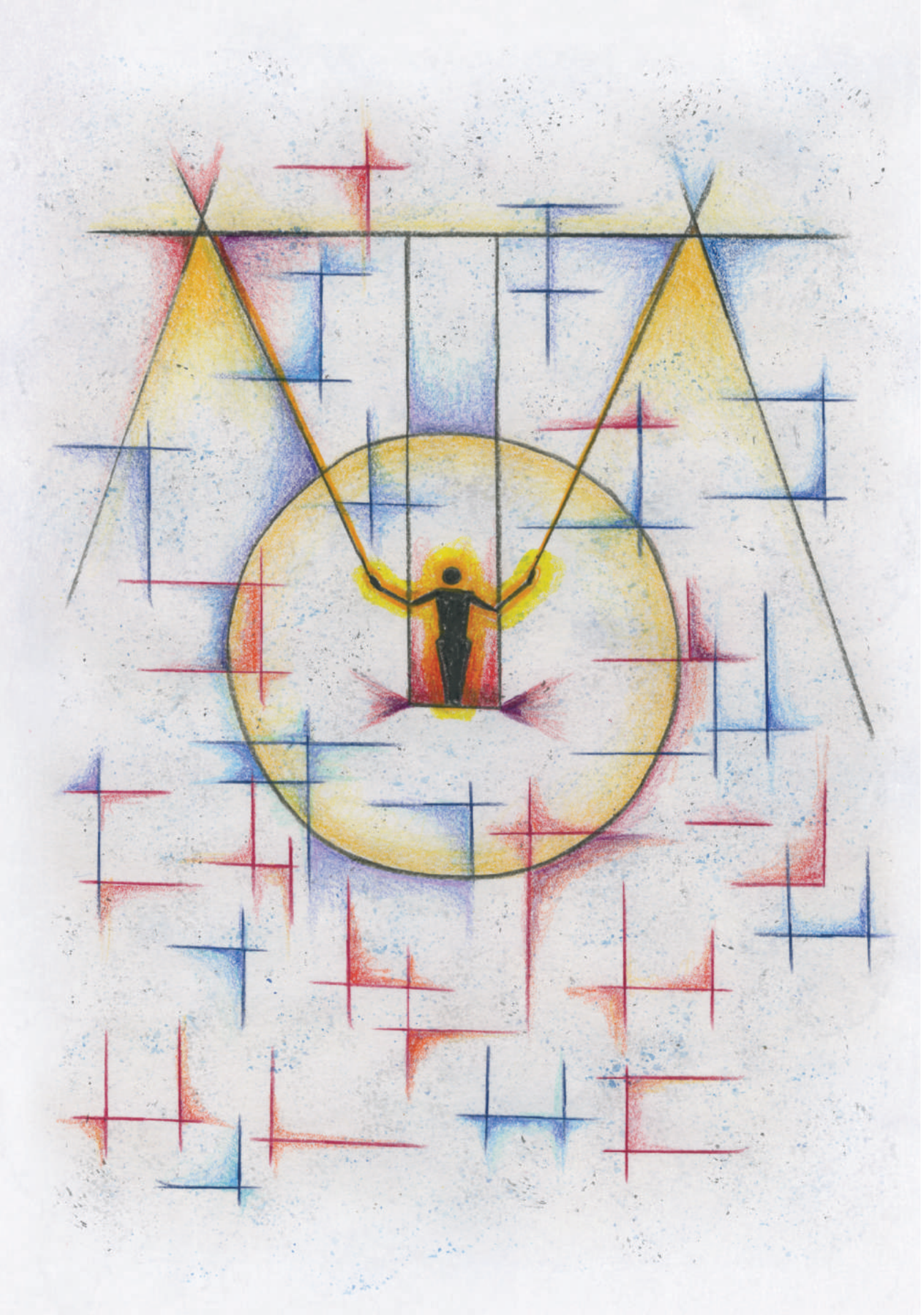
# THE FIELD GUIDE TO IOT SECURITY

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

Booz | Allen | Hamilton

# THE FIELD GUIDE TO IOT SECURITY

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER



# LEARNING THE TRAPEZE **WITHOUT A NET**

As a society, we're rushing into the Internet of Things (IoT) at a breakneck pace, applying it to anything and everything we can think of – cars, planes, and trains, pacemakers, light bulbs, baby monitors, homes, offices, factories, nuclear power plants, electric grids, even children's dolls. If something can be connected, we're connecting it.

The only trouble is, we're moving to IoT faster than our ability to secure it. And IoT is not like traditional IT. It's far more vulnerable to attack. If cyberattackers get control of one of your systems, they can do far more than steal emails and credit card numbers. They can make the "things" in the Internet of Things go wrong. Pick something in IoT, and then imagine what would happen if foreign countries, cybercriminals – or just hackers looking for attention – had their way with it.

**We're simply not ready.**

It's like learning how to become a trapeze artist without a net, without even knowing what the net would look like. But there's no going back. As a society, we're not going to say, "Time out, let's spend the next three years figuring out how to secure IoT, then we can jump back into it." That's not going to happen. Our headlong charge into IoT is nonstop. No one wants to miss the opportunities IoT has to offer, the new products, the new efficiencies, the promise of "smart" everything. No one wants to be left behind.

And here's the rub: If you move into IoT too fast, before you've secured it, and something *does* go wrong – let's say, wrong enough to make headlines – then everything you're trying to do with IoT will unravel. IoT is built on trust, and if people don't trust you, forget it.

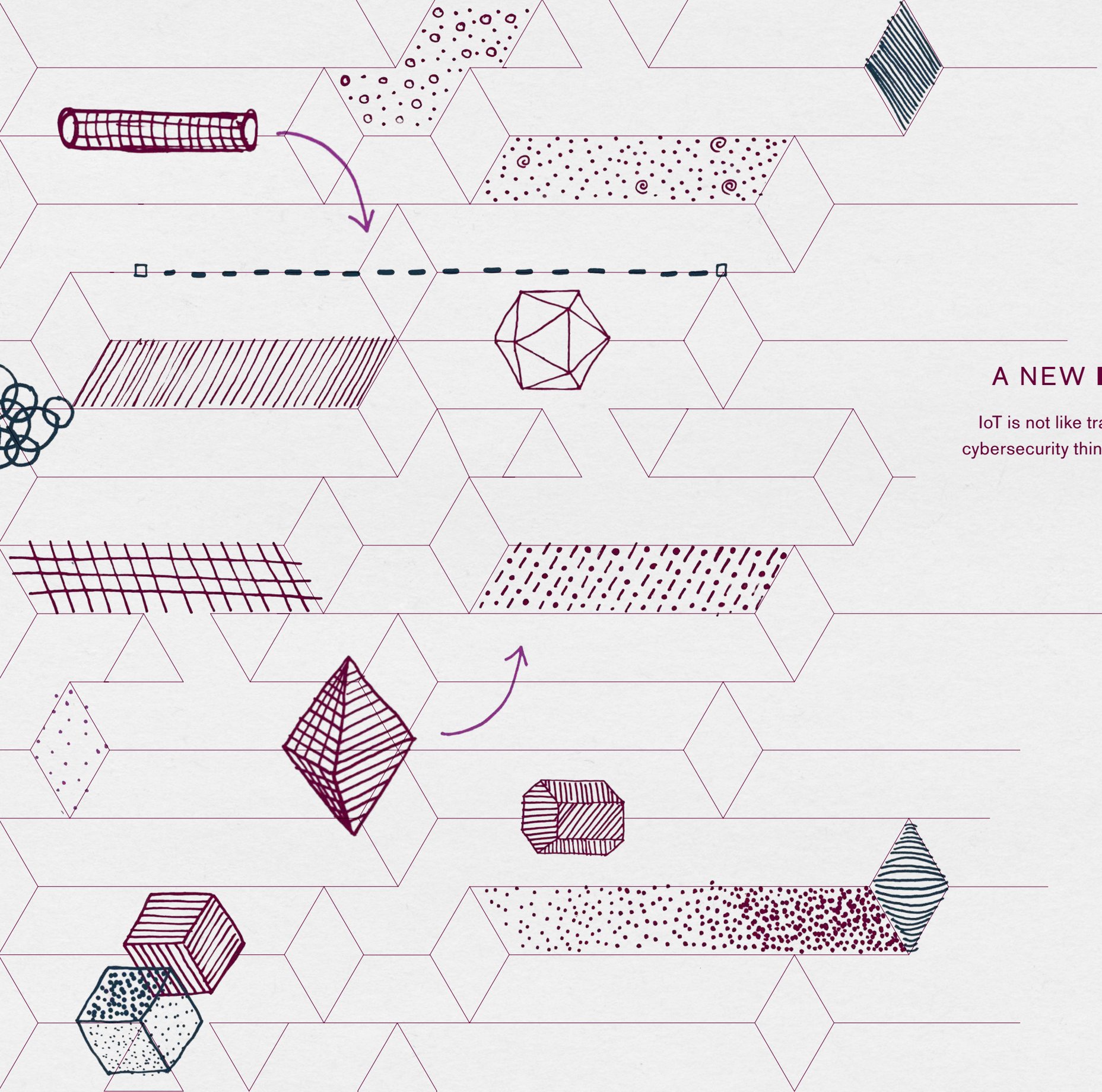
IoT is here, and the last thing you want to do is slow down. So the question is, *Can you be in the forefront of IoT and be reasonably safe at the same time? Is it even possible?*

The short answer is, Yes.

But...and there *is* a but...you'll have to work hard at it. You'll have to do some serious thinking and planning.

It can be done. This field guide will show you how.

# TABLE OF **CONTENTS**



## A NEW **PERSPECTIVE**

IoT is not like traditional IT - and traditional cybersecurity thinking can only take you so far.

# WHY IOT IS DIFFERENT **IN A BIG WAY**

The Internet of Things is not your father's IT. It's not even *your* IT of ten minutes ago.

One reason we badly underestimate the risk is that we believe IoT is just an evolution of traditional IT. Sure, we think, maybe it's IT on steroids, but aren't the principles the same? You just think about it in the same way that you think about your regular IT, right?

Not even close.

The Internet of Things is a completely different animal. With traditional IT, systems are generally closed and self-contained and so easier to protect. But IoT connects your systems with tens of thousands of sensors and other devices that are out there in the world – and often out of your direct control.

## Too Many Doors

Every one of these devices is a potential door for attackers. And not just the devices themselves but also the wireless signals that send the data back and forth and even the apps that run on the devices. Compared to traditional IT, there are exponentially more ways into your systems with IoT. You have to defend all the potential doors, while an attacker has to get through only one.

One of the problems is that many of the IoT devices used today aren't even being designed with security in mind. The idea is, get them made, get them out the door, and get them up and running. Hey, we're in a hurry – we'll worry about security later, and anyway, the risk isn't that bad, right?

There's more. Many of the tiny sensors that are the nerve endings of IoT tend to have just enough processing power and memory to do their jobs. They're not smart enough to decide on their own whether to accept a command or execute a task. And they're mostly automated, with no humans around to keep an eye on things.

It's like living in a house with a thousand doors and no way to put a lock or security camera on each one.

Protecting IoT requires a new perspective, a new way of thinking about cybersecurity. That's what this Field Guide is all about.



# YOU MAY BE MORE VULNERABLE **THAN YOU THINK**

There's no getting around it: IoT security is more complex than it might seem. That's because the vulnerabilities of IoT have a way of sneaking up on us, appearing in places we least expect to find them. If you use IoT, here are a few of the ways you might be caught unaware:

Your IoT systems might be connected in ways you don't realize. In one of the largest IoT breaches to date, attackers used the stolen credentials of an HVAC vendor to get into Target's computerized heating and cooling software. They then burrowed their way into the retailer's in-store cash register systems – where they stole the credit and debit-card data of 40 million customers.[1]

You may not realize that some of your sensors were never designed for high security. A sensor intended for a fish tank isn't likely to offer much protection against cyberattackers.

You might be collecting and transmitting data that you're not even aware of. Many sensors are designed to collect multiple types of data. Even if you only use a sensor for one purpose – say, to measure room temperature – it may be automatically gathering lots of other information. And any of it may be valuable to hackers.

You may have excellent security, but what about your vendors? And what about their vendors? It's not just your own supply chain you have to worry about – it's everyone else's.

You can't fully control the human factor. Despite your best efforts, IoT users might fall for phishing scams, or employees might access your system with unauthorized – and hackable – devices.

**WHAT IS IOT?**

There are many definitions of the Internet of Things. In this Field Guide, it refers, quite simply, to the idea of connecting all manner of devices to networks – through the Internet – to make them "smart." These might be consumer devices, from refrigerators to fitness trackers, or industrial control sensors and actuators. They might be connected cars, or smart buildings, or medical devices like pacemakers and insulin pumps. There seems to be no limit to IoT. It's fast becoming part of every industry – and nearly every aspect of our daily lives.

# THE **SOCIAL CONTRACT**

The Internet of Things is founded on a mostly unspoken – but iron-clad – social contract. And you ignore it at your own risk.

Every user – whether consumer, employee, business or government agency – trusts that your IoT products and services are absolutely safe and will fully protect their privacy. It's a social contract because it's rooted in how we deal with each other in society. *I trust you not to harm me.*

This might seem obvious, but it can easily be forgotten in the rush to IoT. As a society, we seem far more interested in what IoT can do for us than how it might go wrong. We can't wait to join the IoT revolution, to find out how it can transform our lives and our organizations. Who wants to focus on the downside?

But don't be fooled. The social contract is always there, just below the surface. Despite appearances, people's concerns about safety and data security far outweigh their endless fascination with the shiny new objects of IoT. Don't believe it? If users feel that the social contract is broken, you'll get a different kind of user perspective. One that could show up as the first result of an online search of your organization's name.

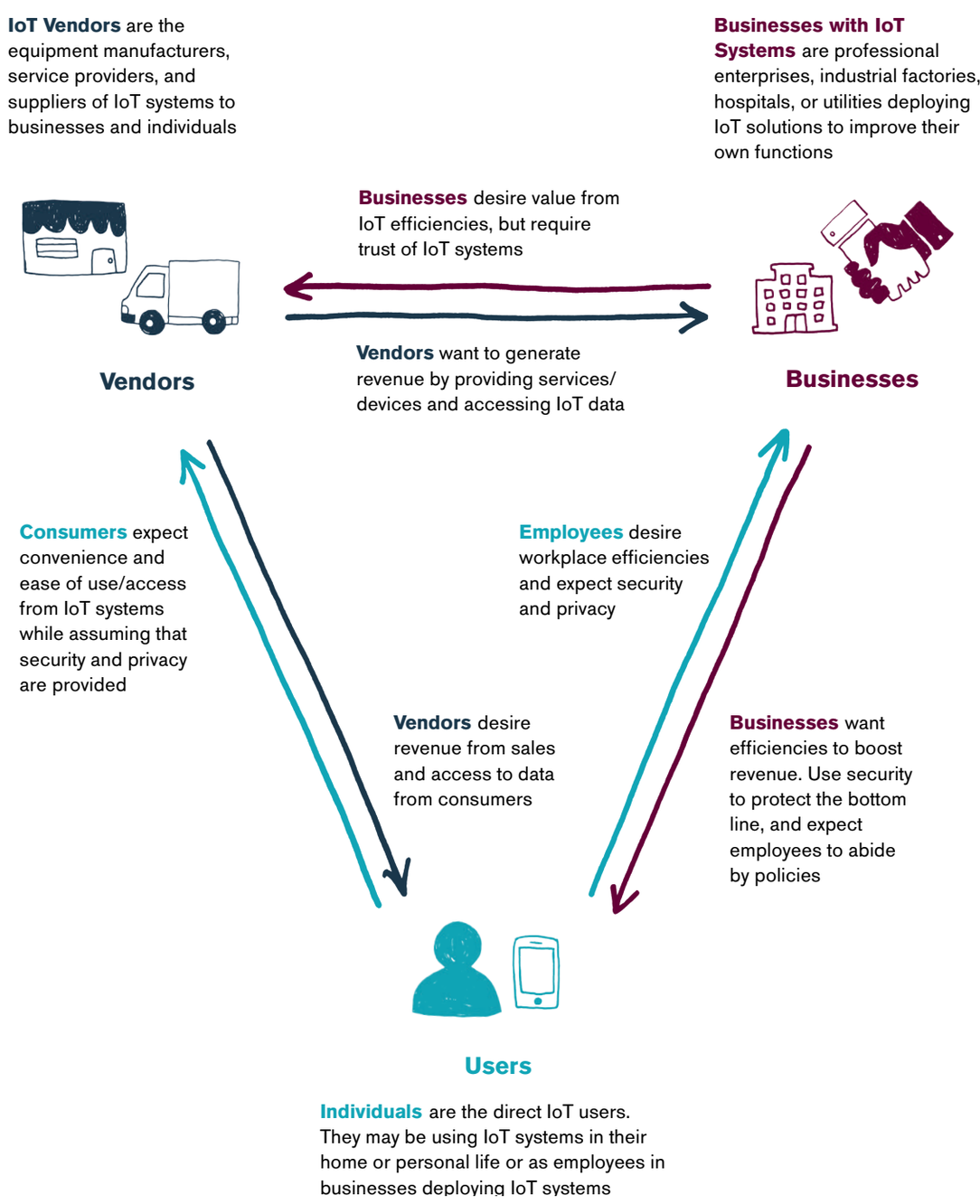
What this means is that you have to do the thinking for the users, whether they are individuals or organizations. You have to look out for them, even if they don't seem to be looking out for themselves. Every decision you make with IoT has to be viewed through the lens of the social contract. What are all the ways that things could go wrong? How are users likely to respond? How would you react, if you were in their position?

Your IoT users trust you, even if they don't explicitly say so, even if they don't demand to see exactly how you're protecting their privacy and safety. In IoT, that trust is everything.

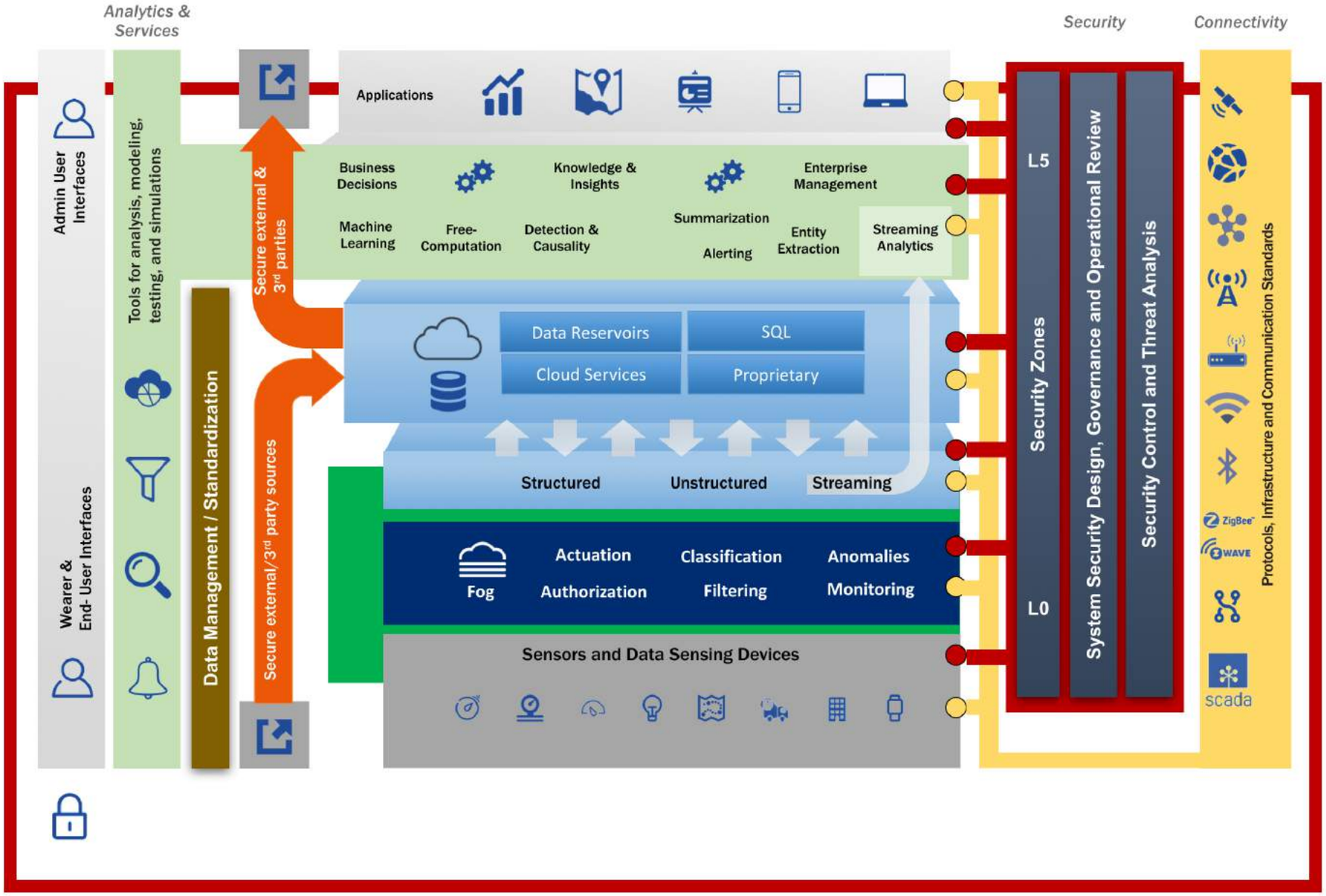


### How the Social Contract Works

The interlocking goals and expectations of the three stakeholder groups in IoT - vendors, businesses, and users create a web of implicit relationships.



## IoT Reference Architecture




Visualizing the complex interconnections and intricacies of IoT can help identify where potential weaknesses and vulnerabilities may lie, guiding your security efforts. This illustration of Booz Allen's IoT reference architecture depicts the fundamental elements of IoT and their interconnections. Together, they make up the technology and process layers that make it possible to collect data from the physical world and turn it into insights for users. Elements include sensors and other devices, edge computing, data repositories, analytics, applications, data management, connectivity (in gold), and the necessary security (in red). Both connectivity and security are present in every layer.

# WHAT TRUE IOT SECURITY **LOOKS LIKE**

The IoT threat landscape changes faster than the weather. The nature of the beast is that you never reach a point where you just say, “We can stop now, we’ve done enough.” However, it is possible to paint a picture of what a well-thought-out, risk management–based approach to IoT security looks like.

It starts with knowledge – about how IoT is vulnerable, about who might try to attack us, and about what could happen if they succeed. Just getting a thorough understanding of all this is half the battle. Organizations with the best IoT security chart all the ways attackers could gain entry into their system – and cause problems – through ‘edge’ devices, communication channels, and IoT’s complex web of interconnections (see the prior illustration of Booz Allen’s IoT Reference Architecture). These organizations also understand who might target their IoT systems – whether nation-states, terrorists, cybercriminals, hacktivists, or insiders – what they could be after and how they might launch an attack. Just as important, the organizations have thought through all the nightmare scenarios of a successful attack – what might happen if sensitive data were stolen, or connected devices were turned against their users.

True IoT security calls for regular risk assessments to determine just how likely you are to be attacked, and how well you’re prepared to defend yourself. Risk assessments also look at the implications of each potential attack, including reputational harm, lawsuits, and regulatory penalties. This exercise makes it possible to take the next step – prioritizing your resources. What parts of your IoT systems should you shore up first? What should be your long-term strategy?

## Going the Extra Mile

Organizations with the best IoT security are proactive – they expect the unexpected, with real-time threat-assessment data that shapes decision making. They use the latest advances in analytics to spot hidden IoT attacks. And they’re ready for that worst-case scenario. They have plans in place that bring together the entire organization – not just the technical side but experts in crisis communications, marketing, compliance, and legal issues.

Perhaps most important, such organizations honor the social contract. Everything flows from there. This helps make sure that security is always “baked in” to their IoT – from every phase of the lifecycle to governance and policy. IoT security is in their DNA.



# MAKE SECURITY PART **OF YOUR IOT DNA**

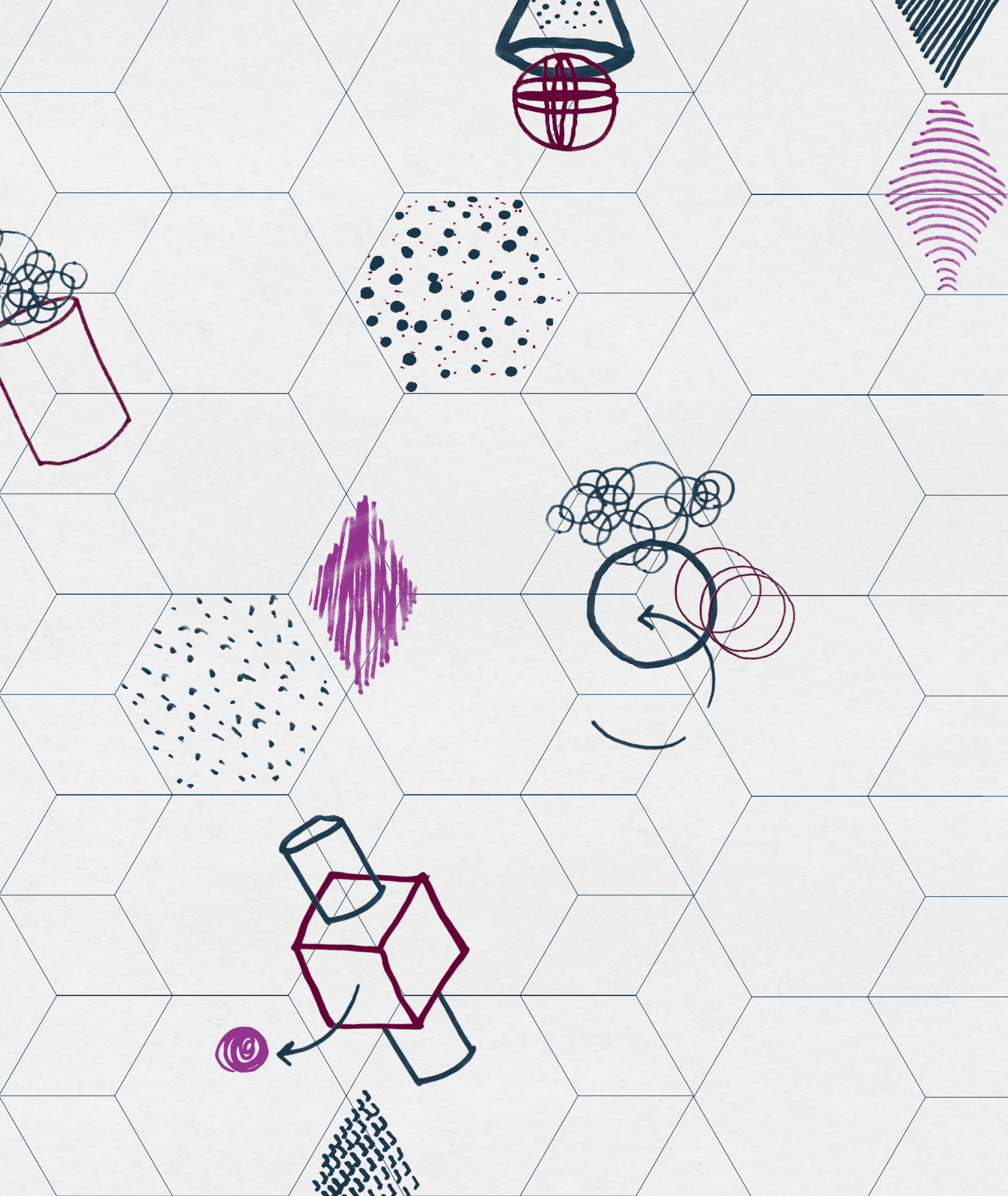
If you want the trust of users – in other words, if you want to succeed with IoT – security has to pervade your thinking. It has to be part of your organization’s Internet of Things DNA.

If you’re in the C-suite, you can’t delegate this. Your organization needs a top-down commitment that security is essential to every aspect of IoT. And it needs that commitment to be followed through in every business unit, every department, every cubicle.

If you’re in IT, or play any other role in the Internet of Things, be an enthusiastic advocate for security. Campaign hard for it at every meeting and in every idea, every proposal, every prototype. Be known for it. Make it yours.

### Key Takeaways:

- It is easy to underestimate the IoT security risk because we believe IoT is just an evolution of traditional IT. But with IoT, there are exponentially more ways into your system – and so the risk is exponentially higher.
- If providers of IoT services or products violate the often implicit social contract and betray the trust of users – their entire IoT effort could fall apart.
- True IoT security requires a proactive approach that fully considers the risks and implications of attacks, and then builds in comprehensive protections from top to bottom.
- Security can’t be an afterthought – it has to be part of everything you do with IoT.



# UNDERSTANDING YOUR **VULNERABILITIES**

You need to know who and what you're up against. Because forewarned is forearmed.

# NEW **WEAKNESSES**

*The Risks of a More Open and Complex System*

One of the most daunting tasks in IoT security is simply understanding all the ways you're vulnerable. With conventional IT, a massive body of cybersecurity knowledge has been compiled over the years – we know a great deal about how we can be hacked and what the attackers can do. But with the Internet of Things, much of that hard-won insight has to be rethought.

It's not that cybersecurity technology isn't there – in most cases, it is. It's that we often don't fully understand where and how we need to use it. And so one of the first steps to IoT security is to shine a light into all the dark cracks of IoT to see where attackers might slip in. This involves a close, careful, systematic examination of all potential weak points. But it also requires imagination – the ability to get out of our traditional ways of thinking about cybersecurity and see our IoT systems through the attackers' eyes.

IoT is more vulnerable than traditional IT in three key ways:

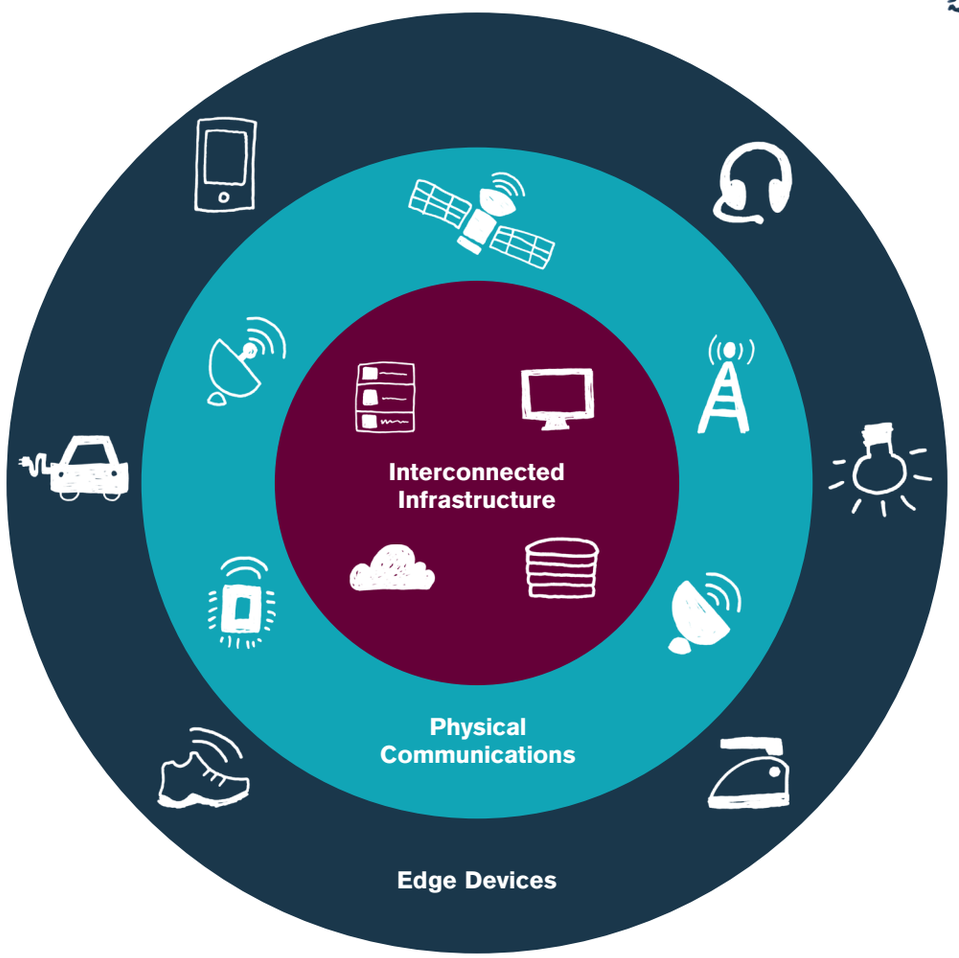
- Through **edge devices** – the "things" of the Internet of Things
- Through the wireless and wired **communications** that shuttle information back and forth
- Through the complex **interconnections** that bring IoT systems together

IoT makes each of these areas far more open to attack than before. And so you must approach each with a new mindset.



**Key Vulnerabilities of IoT**

The complexity and connectivity inherent to IoT introduce new security vulnerabilities.



## Edge Devices

The great paradox of IoT is that what makes it possible – our ability to put sensors on just about everything – is also what makes it inherently difficult to secure. Many of the estimated 15 billion sensors and other edge devices in use today simply do not have sufficient protection from attack.

That danger was vividly illustrated in October 2016, when hackers commandeered hundreds of thousands of DVRs, baby monitors, security cameras, home routers, and other devices to launch distributed denial-of-service (DDoS) attacks that crippled major websites such as Twitter, Reddit, and Airbnb. The hackers took control of the devices by using a malware known as *Mirai,* which guessed at their simple factory-set passwords, such as *admin, 12345,* and even *password*.[2] The incident was a wake-up call that everyday IoT devices, if unprotected, can be used to bring down parts of the Internet.

But weak passwords are just one facet of a broad range of vulnerabilities in sensors and other IoT devices. Part of the problem is that until the recent spread of IoT, there has never really been a need to equip sensors with high levels of cybersecurity. They've long been part of modern technology – registering temperature, light, pressure, movement, and other attributes of the physical world. As long as they weren't connected to the Internet, security wasn't much of an issue.

However, they are being connected now - and there is a growing awareness that they're not up to the challenge. Many sensors used in IoT these days, particularly in industrial control systems, were never intended to be connected to the Internet. Even some new sensors don't have the security necessary for IoT – with few exceptions, sensor manufacturers are more focused on providing commercial products quickly rather than securely. IoT systems often end up with a mix of sensors that are more or less secure – and it's not always easy to tell the difference.

Hackers can gain control of a sensor by physically altering it (perhaps even replacing it with a phony one) or by manipulating it remotely. Either way, sensors can be hard to protect. They are generally "in the wild" – outside the traditional ring of cybersecurity defenses. In particular, many simple sensors are difficult to manage remotely, because of their low power and potential intermittent connectivity. Additionally, many of these simple sensors are only able to send information to the data stores, and don't have the ability to receive back configuration instructions. If there's a security flaw, it's hard to update them with security patches or other fixes – and impractical to replace them by the tens of thousands.



## Communications

In thinking about how your IoT connections can make your system vulnerable, it can be helpful to divide them into two types. There's the back-and-forth flow of data between the "edge" devices and the central system. And there's the flow of data within the central system itself. Each type has unique challenges in IoT.

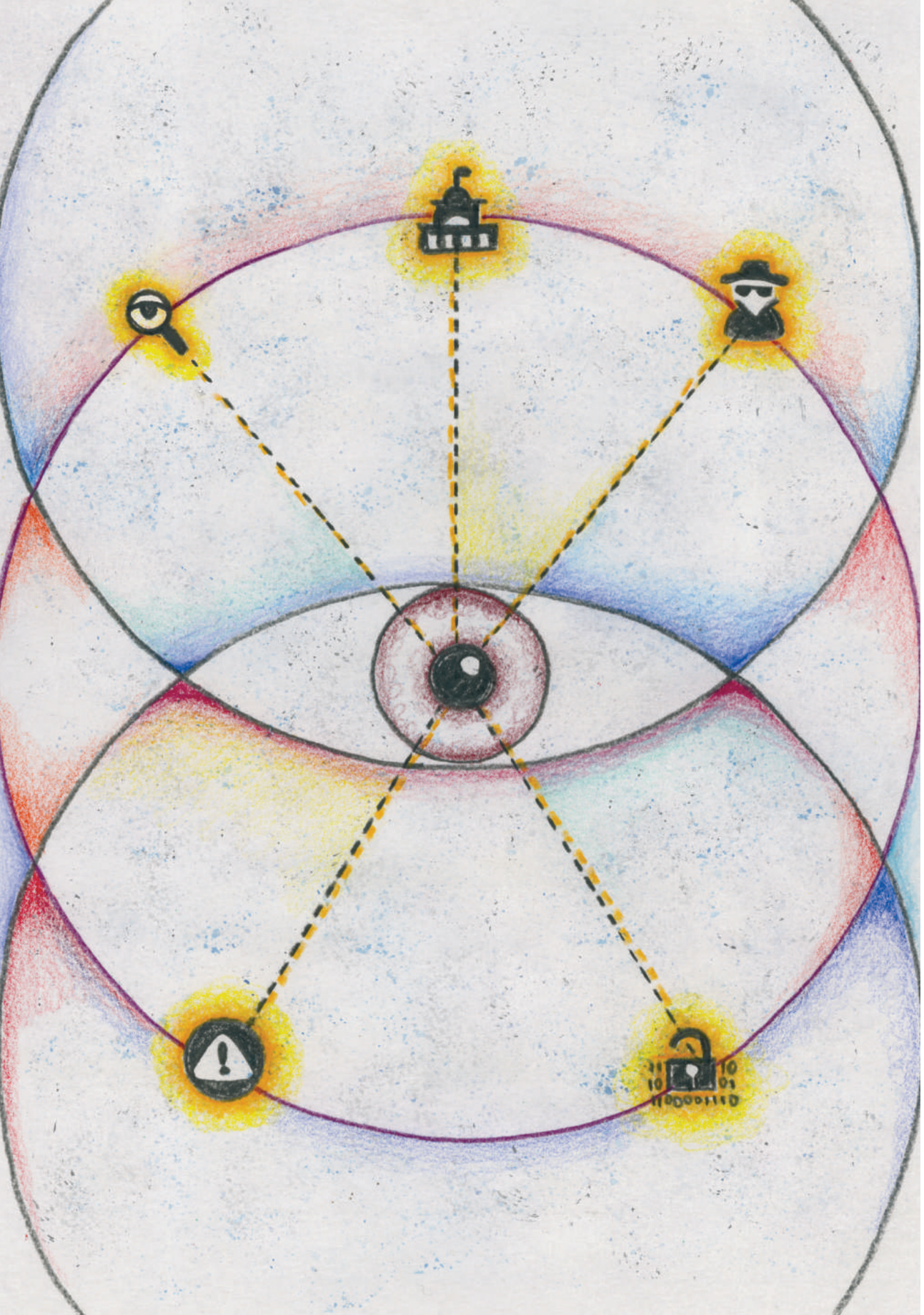
IoT at the edge is a never-ending rush hour of wireless and wired data traffic. Sensors are constantly sending out signals to gateways that collect and organize the data. The gateways are exchanging that data with other devices on the edge and with the central system's cloud platforms, where the data is analyzed. And without proper safeguards, all of this traffic is open to attack.

Hackers who intercept wireless signals at the edge can steal data without you realizing it. They can insert their own data into the traffic stream and give misleading information to users or tell IoT devices to do things they shouldn't. One example is the "man-in-the-middle" scheme, in which a hacker breaks direct communication between two devices in a data conversation and impersonates both. The two devices still think they're talking to each other, but it's really the hacker giving them false information and telling them what to do.

## Interconnections

Organizations typically bring together and analyze data from a wide range of sources. This often means connecting parts of the IT network that were never connected before – and perhaps were never intended to be. Connections within the system can become increasingly porous, without the organization being aware of it – particularly when the flow of data is automated.

The danger, of course, is that if hackers get into one part of your IoT, they may have access to it all. There are many ways they might get in: through a sensor, through a third-party vendor (like the Target attackers), through an employee who sets up his or her own wireless hotspot in violation of company policy. All they need to do is find a weak point – a part of the system that has a lower level of security – and they'll get a free ride through all the unguarded interconnections.





# MEET YOUR **OPPONENTS**

*Who Will Attack Your IoT, and How Will They Do It?*

Who are the people who might want to steal your data or manipulate your IoT devices? What would be their motivations – what could they gain by attacking you? Have they attacked IoT systems like yours before? How successful have they been? These are all questions you need to think carefully about as you plan to defend your IoT. Those who might do you harm are already out there. And you need to know exactly who and what you're up against.

Five type of hackers threaten the IoT – nation-states (or state-sponsored attackers), terrorists, cybercriminals, hacktivists, and insiders. Each type has its own range of motivations and capabilities.

## Nation-States and State-Sponsored Attackers

Foreign governments may want to steal data as part of intelligence or military operations. Or, they may try to help their country's businesses through industrial espionage or intellectual property theft. There is also the danger that nation-states will launch cyberattacks to disrupt critical infrastructure – as with the kind of attack, possibly by Russian hackers, that brought down Ukraine's energy grid in December 2015.[3] Nation-states typically have a higher degree of both funding and capability than other groups.

## Terrorists

U.S. officials are becoming increasingly concerned that terrorists could use connected devices to carry out attacks. According to FBI Director James Comey, terrorist groups have begun discussing ways to hit Americans with a cyberattack. Although Director Comey has not specified what terrorists might try to target, U.S. officials have been stepping up efforts to protect America's critical infrastructure, including water-treatment plants, electrical grids, and the banking system.[4]

John Carlin, the U.S. Assistant Attorney General for National Security, has warned that attacks like the one in Nice, France, in July 2016, in which a terrorist driving a truck mowed down and killed 84 people, could eventually be launched remotely. Said Mr. Carlin, "If our trucks are running in an automated fashion — great efficiencies, great safety, on the one hand — but if we don't think about how terrorists could exploit that on the front end, and not after they take a truck and run it through a crowd of civilians, we'll regret it."[5]

## Cybercriminals

Because IoT lacks the hard outer shell of traditional IT, it is a particularly inviting target to cybercriminals. Whether in small groups or as part of large criminal organizations, they are becoming increasingly creative and sophisticated in finding ways to profit from cybercrime. A global criminal ring, for example, stole $45 million from thousands of ATMs around the world, including from nearly 3,000 ATMs in New York City.[6] Cybercriminals will steal any kind of data that they might be able to resell, from credit card and Social Security numbers to proprietary company information. They also steal and sell IoT network passwords and other credentials, including to the systems used to control infrastructure and industrial processes. IoT presents broad opportunities for cybercriminals to extort ransom - for example, by manipulating devices on a shop floor.



## Hacktivists

IoT hacktivists are bent on damaging an organization's reputation. In addition to launching DDoS attacks, they are increasingly stealing and releasing embarrassing information about organizations and their employees. In addition, with the IoT, organizations collect vast amounts of personal data from customers. If that information is stolen and made public, it could derail the organization's IoT efforts and damage its overall reputation.

## Insiders

The threat from insiders may be the most insidious of all. They not only have access to the systems and networks, they know these systems' weak points, their hidden ways in. Malicious insiders are typically disgruntled employees or are motivated by the desire for financial gain. They can also be hacktivists. Insiders may want to make money by selling stolen data or by working on behalf of outside attackers. Insider attacks are among the most difficult to detect.

Insiders can also inadvertently open the door for outside attacks, by falling for phishing and other schemes. One common trap is the "watering hole," in which attackers set up a phony website that looks like one commonly used by the employees they're targeting. When the unsuspecting employees intertact with the website, it downloads malware onto their computers.

## Pinpointing Who Might Attack You – and Why

A good way to get a sense of your own risk is to carefully examine the attacks your industry peers have faced. What did the hackers target? What were they trying to accomplish? Here, you're not just hypothesizing about what hackers might be interested in doing – you're identifying areas where they've already demonstrated an interest.

Next, look at what methods they used in their attacks. Which tactics and techniques did they prefer? Which were most successful? Studying what worked for attackers – and what didn't – can provide insight into your own strengths and vulnerabilities.

## Potential Attackers and Their Motivations

Understanding the motivations of the various types of attackers allows you to more accurately assess the likelihood and risks posed by threats from the perspective of your organization.

| | State Sponsored | Terrorist | Cybercriminals | Hacktivist | Insider |
|---|---|---|---|---|---|
| **Intent** | Nation-states and state-sponsored attackers seek to conduct industrial espionage or intellectual property theft, disrupt critical infrastructure, or interfere with political processes. | Terrorists seek to cause loss of life or financial panic. | Criminals try to gain financially by stealing information or by extorting money from individuals and organizations. | Hacktivists seek to promote a social, political, or ideological cause by damaging an organization's reputation. | Malicious insiders typically hope to satisfy a grudge, or gain financially by selling information. Insiders can also inadvertently launch attacks when manipulated by outside attackers. |
| **Example** | In December 2015, Ukraine's public energy grid was temporarily disabled, possibly by Russian hackers. The attackers gained credentials via spear phishing, established remote access via a virtual private network, and used administrator services to access the control network. | In March 2016, three members of the "Syrian Electronic Army" were accused of gaining credentials to the Twitter account of the Associated Press and tweeting a false news alert that there were explosions at the White House and that President Obama was injured. | In spring 2016, the Lansing, Michigan, Board of Water & Light paid a $25,000 ransom to unlock its internal communications systems after they were disabled by a cyber attack. An employee had unknowingly opened an email with an infected attachment. | In 2005, hackers associated with the Anonymous movement stole more than 1,000 email credentials from five multinational oil companies and dumped them online. | An Australian employee at Maroochy Water Services accessed the company's Supervisory Control and Data Acquisition system and released millions of gallons of sewage spill into waterways, hotel grounds, and canals around the Sunshine Coast suburb. |
| **IoT Challenge** | Many IoT devices are manufactured overseas and may be subject to tampering by state-sponsored attackers. | Terrorists do not need to fully destroy critical infrastructure to achieve their ends: Simple disruptions can spread fear and financial panic. | Criminals are attracted to IoT by the vast amounts of data collected as well as by the growing number of unprotected consumer devices. | Legacy devices that are no longer associated with the organization may contain personal data or proprietary information, both of which are of high value to hackivists. | With the proliferation of edge devices, the number of manufacturers, vendors and other third parties is increasing exponentially. |

# HOW ATTACKERS COULD EXPLOIT YOUR **DEVICES AND DATA** *What's the Worst That Could Happen?*

Our rush to IoT is built largely on faith – faith that what could go wrong probably won't because we'll have enough cybersecurity. And so we're putting devices online by the millions without fully considering what attackers might try to do. But is faith enough to bet the safety and privacy of your users and the reputation of your organization?

It's essential to think through all the worst-case (or just plain bad-case) scenarios. If somebody got hurt or critical data were stolen, how could it damage your reputation? What kinds of regulatory penalties could you face?

## How Your Devices Might Be Misused

It's both easy and hard to imagine what could happen to your **devices**. Easy, because the most obvious things hackers might do have been well studied and debated. Hard, because the hackers are always coming up with new ideas. And so you have to beat them to it, by systematically thinking through every possible way even the most innocuous IoT devices could do you or your users harm.

There are other angles to consider. The recent DDoS attacks using DVRs, baby monitors, and security cameras raises the possibility that your devices might be compromised and used in attacks on other organizations. With the increase in bring your own device (BYOD) scenarios, there's also a growing risk that attackers could misuse your employees' smartphones and other devices, as well.

## How Your Data Might Be Misused

IoT **data** misuse is also more complex than it might seem. It's not enough to think about how your raw data could be misused. What about all the data you're correlating? How could hackers take advantage of the many connections you're making? And there is still another hidden vulnerability in IoT – what about the ways hackers might correlate the data themselves?

If hackers gain access to your IoT systems, they may be able to bring together disparate data sources that you never intended to combine and perhaps wouldn't want to. By correlating different types of data, for example, hackers may be able to gain personal information about your IoT users and target them for identity theft. Or, they may be able to gain proprietary or embarrassing information about your organization and how it operates.



IoT, with its constant, automated collection of vast amounts of data, presents a fat target for hackers. There's much more data to go after than with traditional IT – which means bigger payoffs for hackers if they're successful. To fight this increased threat, it's important to get a handle on not just where all your data is but how easy or difficult it would be to combine. Then, think through what those combined databases might reveal. Don't forget to consider how your data, if stolen, might be correlated with data from outside sources. Could it somehow make your users more vulnerable?

### Key Takeaways:

- Until recently, there wasn't a need to equip sensors and other edge devices with high-level security – and as a result, many don't have the safeguards needed for the IoT.
- IoT brings together different systems that were never connected before – and perhaps were never intended to be. As these connections grow, they can make you increasingly vulnerable without you being aware of it.
- The five common types of IoT attackers – nation-states, terrorists, cybercriminals, hacktivists, and insiders – have different motives, methods, and targets. A good way to understand your own risk is to study the attacks on your industry peers.
- Take the time to think through how your data and devices could be misused, and the potential implications, including reputational damage, lawsuits, regulatory penalties, and other financial harm.

# THE BUILDING BLOCKS **OF IOT SECURITY**

Creating a strong, living security framework.

## The Building Blocks

### 1 Assess Your Risks

- Assess vulnerabilities and threats.
- Calculate risks and determine likelihood.
- Enumerate risks that have business impacts.
- Prioritize mitigation plans.

### 2 Develop a Strategy

- Use a standardized process or risk assessment framework.
- Incorporate blended teams of industry-specific subject matter experts
- Decompose environment to critical components and communication paths.
- Characterize your attack surface.

### 3 Employ Proactive Threat Detection and Prevention

- Deploy security based on informed (risk-based) decisions.
- Practice the basics.
- Take a proactive approach.
- Red Team yourself; don't assume it works.
- Validate to confirm deployment and compliance.

### 4 Prepare for Incident Response

- Prepare for cyber incidents and have a communicated plan.
- Manage the incident with engagement of all stakeholders.
- Rebuild deliberately after the event.

A strong framework for implementing IoT security is built around four basic elements. You can use these four building blocks to develop your own framework, but it's not enough to just roll out a new plan. Security is a cultural change. It has to become part of your IoT DNA.

# ASSESSING **YOUR RISK**

*Where Is Your System Vulnerable?*

One of the key building blocks of IoT is a risk assessment, which takes a careful look at your current defenses. How well are you prepared, right now, to deter and respond to attacks?

## Laying the Groundwork

It's important to have the right process in place for a risk assessment. That process can and should be based on industry standards, such as from the National Institute of Standards and Technology (NIST), as well as on governmental and international policies. But a one-size-fits-all assessment won't work in IoT. No two IoT systems are alike, and many organizations have multiple IoT systems with unique architectures. Each system and each architecture needs a tailored approach.

The way to achieve this is by reaching out to your key internal stakeholders, and working with them to build the risk assessment process. Through this collaboration, you can answer such questions as, Whose role is it to find the risks in your IoT systems? How do you evaluate any vulnerabilities you find – what kind of scoring system should you have? Whose responsibility will it be to plug the holes? How will that work be approved and funded?

All these questions can't simply be raised – they must be fully answered *before* you begin evaluating your IoT system. Otherwise, the risk assessment will be haphazard, and any problems that you find may end up only half-addressed. If you're going to look for trouble, you have to be ready when you find it.

## Probing for Weaknesses

Begin the risk assessment by creating a detailed map of your IoT systems. Such a map identifies every edge device that connects to your networks and its level of security. The map also details your communications channels as well as your system's complex interconnections.

The next step is to develop a comprehensive list of all the ways an attacker could manipulate each of these elements. Don't worry at this point about whether any of it is even possible – the idea is to brainstorm worst-case scenarios. Threat-intelligence reports can help here; you can see what hackers are doing to other systems, and then imagine what could happen to yours.

This part of the process requires the ability to see your system through an attacker's eyes. The hackers are doing the same type of brainstorming – and they can be very imaginative in figuring out ways to create havoc. Think the way they do. And then use that insight to guide your penetration testing, in which you essentially put yourself in the place of the attacker, and see how far you can get. This approach should extend beyond the boundaries of your system, to include your equipment vendors and service suppliers. Where are the specific risks in each aspect of the supply chain?

Next, evaluate the probability that a hacker could actually carry out a specific attack. Some scenarios might be too complex to pull off; with others, getting around your defenses might not be worth the trouble. Hackers are like burglars - they look for easy ways in. If a window is barred, they'll look for one that isn't. By systematically going through all the attack scenarios, you'll gain an understanding of where and how hackers are most likely to succeed and what kind of damage they might do.

## This Is Not One-and-Done

IoT risk assessment is an ongoing process. Everything about IoT is in constant flux – your system and its changing technology, your customers and their evolving needs, your business partners and their fluid supply chains. And of course, nothing changes faster than the attackers' strategies and tactics – for every move you might make, they'll make a move (or two). To keep pace, the risk assessment process needs to be embedded in your day-to-day IoT operations. Just as important, it needs to be highly flexible so that it can reflect the continuous and rapid change of IoT.

# DEVELOPING **A STRATEGY**

*How Should You Prioritize Your Resources?*

It's difficult – perhaps impossible – to fully secure every aspect of IoT. There are simply too many paths of attack, and cybersecurity resources are always limited. This means that you have to focus on securing what's most important. But how do you know where to start? How do you decide?

## Considering the Implications

Knowing how you might be attacked is not enough – just as important in prioritizing your resources is understanding how an attack could hurt your organization overall, particularly financially. Once you've completed a thorough risk assessment, bring together experts from throughout your organization to think through the implications of each potential attack.

The most serious thing that can happen, of course, is that people get hurt by a sabotaged product or IoT device or by a loss of vital services. IoT users can also suffer psychological harm, such as in a close call or when their personal privacy is violated. And they can be hurt financially by a data breach.

Any of these outcomes of an attack could have serious implications for your business. If your reputation suffers, how much business could you lose? How much would your stock likely drop? How would it affect your ability to expand in the market? And there might be other repercussions, as well. If you were sued, what kinds of legal fees and jury awards might you face? What about potential regulatory penalties or restrictions on your future business dealings? What would be the financial or other implications if proprietary information were stolen?

While it may be hard to come up with definitive answers to any of these questions, you can't let that deter you from trying. One type of attack could seem scary but have no lasting impact. Another could come out of nowhere and derail your entire IoT effort. You need to know the difference.

## Understanding Your Limits

To prioritize your resources, you have to be realistic about what you can and can't do. In some cases, IoT decision makers might agree to fix a vulnerability but are overly optimistic about their ability to get the necessary funding. In other cases, one part of an organization may strongly resist certain IoT security controls, arguing that they're not necessary.

Implementing IoT security is just like trying to accomplish anything else in your organization. Internal politics, cost concerns, changes in leadership, and the press of other priorities often make it harder in real life than on paper. Every organization will have barriers to securing its IoT systems. It's important to recognize yours now – before your good intentions hit a brick wall.

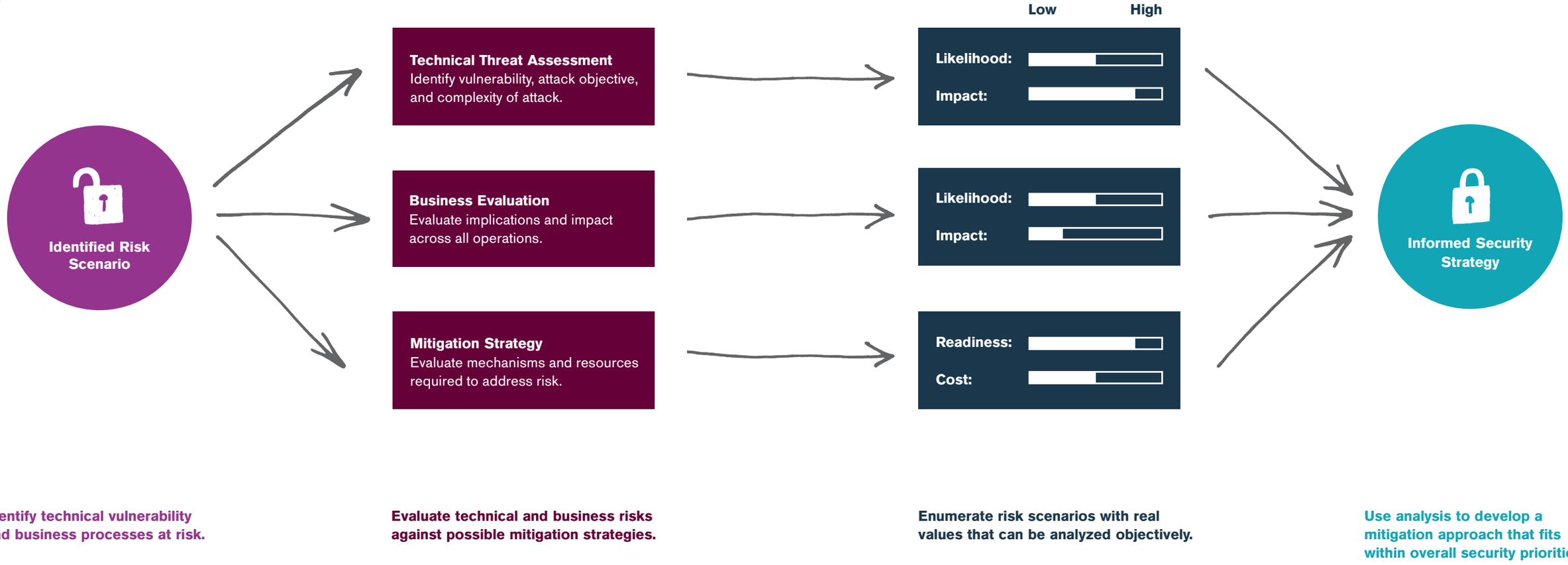
## Building a Resource Prioritization Model

A *prioritization model* considers three elements – the technical risk assessment, the potential impact of an attack on the business, and mitigation strategies. Essentially, the model answers three questions: What could go wrong, how would it affect us, and what can we do about it?

Creating the model is not a top-down exercise. Rather, it's an inclusive process that involves stakeholders from across the organization, including human resources, security, IT, law and compliance, and vendor sourcing. The prioritization model ultimately empowers an organization's leaders and stakeholders to make effective IoT security investment decisions. And there's a secondary benefit: The process of building the model makes sure that disparate teams understand their interdependent risks, technologies, and investments. The model helps serve as a common platform for IoT security dialogue across the enterprise. Once developed, the model becomes a living tool – one that's regularly evaluated, updated, and discussed as part of the organization's broader security processes.

## Resource Prioritization Model

Building a strategy based on informed risk decisions helps leaders determine the areas with the highest return on investment for their security capital expenditures



# EMPLOYING PROACTIVE THREAT **DETECTION AND PREVENTION** *New Approaches*

Traditional approaches to threat detection such as penetration testing are essential to IoT security – but they're not enough. The threat to IoT is simply changing too fast. We need to find a way to detect new kinds of attacks we haven't even thought of. Fortunately, IoT itself helps provide a solution. It brings together a vast ocean of data from edge devices and other sources. And by searching for patterns in that ocean, advanced analytics can spot new and unexpected IoT attacks.

## Too Many Possibilities

In theory, many attacks on IoT should be relatively easy to detect. Over time, you've established normal ranges, or *thresholds,* for your sensors and other devices as they measure temperature, pressure, motion, etc. If a particular sensor reading goes outside the range, you get alerted, and you can check it out. It may be just an innocent malfunction – or it could be part of a cyberattack.

The problem is, there are almost endless ways that sensors can behave, alone and in combination. You may be able to develop ranges for some of those behaviors, and that's an important first step. But hackers are constantly changing their strategies and methods, and they may launch an attack that fails to trigger your established threshold warnings. It's not feasible to plot out in advance each possibility. So, how can you know when you're being attacked?

## The Power of Analytics

Advanced analytics can help, by looking for subtle anomalies in the data that might indicate an attack. The first step is to bring together all the data flowing from sensors and other devices. You can achieve this by creating a "data lake," which has the ability to collect and integrate an almost unlimited amount of data. Then, advanced analytics search through the data for anomalies.

You might see, for example, that all the sensors in a certain group are behaving in the same way. Nothing seems out of the ordinary, but then one of the sensors starts behaving differently from the rest. It's wandering away from the flock, so to speak. Advanced analytics can pick up this subtle pattern change and send you an alert so you can investigate what's happening. And if you discover that a particular anomaly is indeed an indication of attack, you can build it into your system so that you're notified if it occurs again.

With the help of machine learning – in which computers develop a growing awareness of the data – you can build an increasingly complex model of what "healthy" and "unhealthy" behavior looks like in your IoT systems. You're actually doing two things at once. You're using your body of knowledge—all the thresholds you've established – to detect attacks. At the same time, you're building on that knowledge by discovering new ways that sensors and other devices behave when they're under attack. Both activities are equally necessary for a secure IoT. And they make it possible for you to build out your IoT capacity. As you add more sensors and other devices, their readings – and anomalies – automatically become part of the expanding model.

# PREPARING FOR **INCIDENT RESPONSE** *Going the Extra Mile*

Detecting an attack is just the first step. You need to be ready on all fronts should that attack be successful, from resilience to crisis planning.

## Build in Resilience

If attackers get through, how do you close the breach and control the damage without shutting down all your IoT systems? A robust approach requires resilience – the ability to adapt to an attack and keep IoT systems up and running. To achieve resilience, you need to be able to quickly isolate the parts of your IoT systems that are under attack.

An effective approach is to map out your entire IoT beforehand – identifying specific components and determining how they fit together. You can then establish clear rules governing how those components should operate. If these rules are broken – such as in an attack – you can be immediately alerted. Additional rules can lay out how that response should unfold. Who should be notified, and what should they do? If necessary, how should the components be isolated and the attacks contained?

Much of this process can be automated through vulnerability scans, anomaly monitoring and detection, incident-response actions, and other approaches. Resilience can't be improvised once an attack has begun – it must be built into your overall strategy.

## Prepare with Your Stakeholders

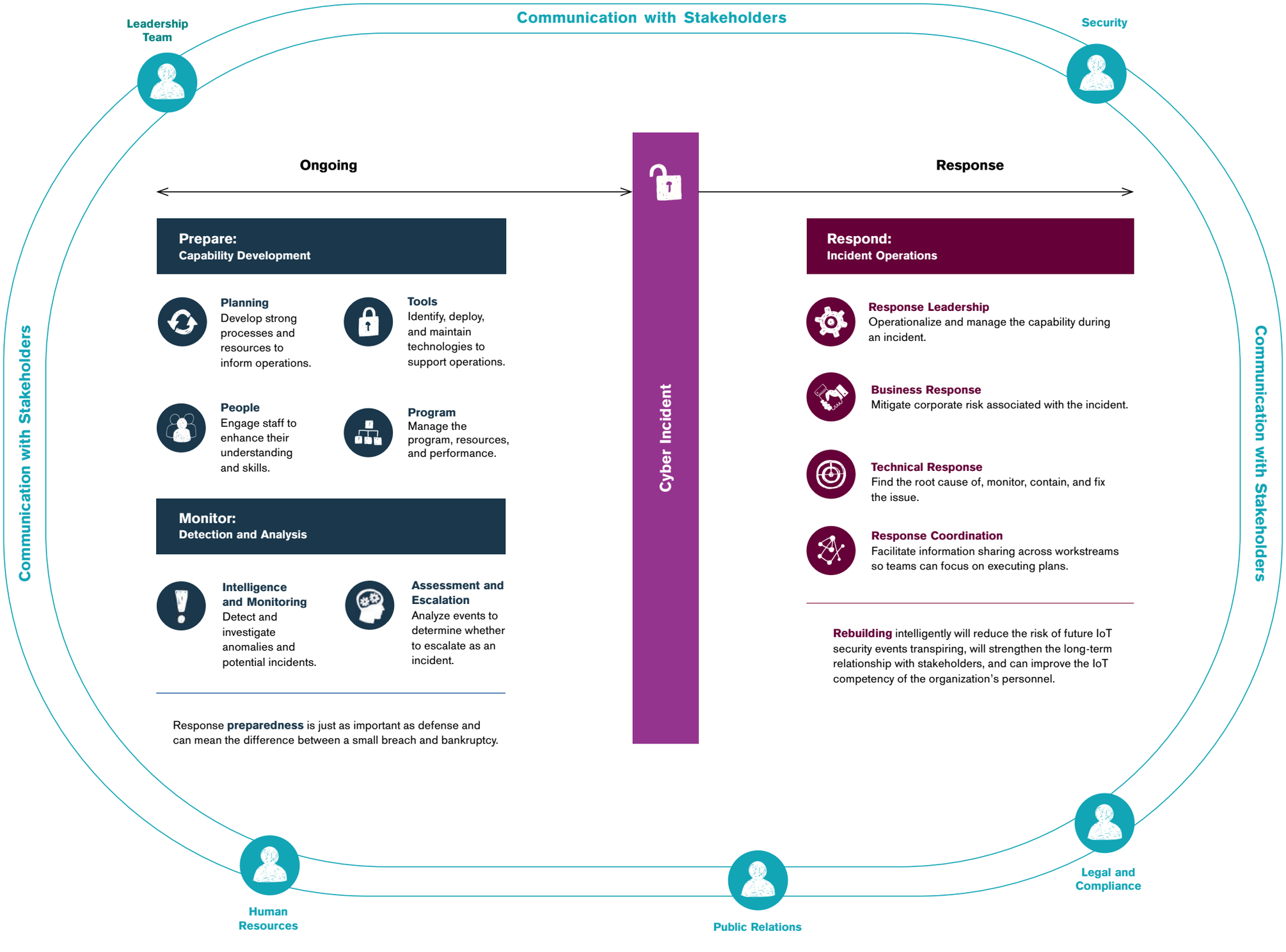
Traditional incident response – rapidly deploying a team to stop breaches, identify additional threats, and restore functionality – is necessary but no longer enough. If you break the social contract, you'll need more than just technical folks to set it right. You'll need experts in crisis communications and marketing as well as help from departments such as Legal and Compliance. Bring all the stakeholders in to develop a response plan – before you need one – and then practice implementing it with scenario-driven exercises. Update the plan regularly, and don't stop practicing and improving. The threat to IoT is moving fast, and if your plan just sits on a shelf, it may not be much help when you need it.

## Don't Stop with Compliance

Many organizations look at incident response through the lens of compliance. Have we checked all the boxes? If there's a successful attack, will we be able to say that we did what was required? With IoT, a simple nod to compliance is no longer enough. People who have been burned – customers, employees, business partners – won't care much whether you met certain "standards." They'll see a failure on your part as a betrayal, and they'll hold you accountable. The worst that could go wrong just might, and you need to be ready.

## Key Elements of Incident Preparation and Response

An effective incident response requires ongoing preparations and regular communication with stakeholders.



# MAKING THE BUILDING BLOCKS **PERMANENT** *How Security Becomes Part of Your IoT DNA*

As a society, our IoT philosophy up to this point has been, "Connect first, and ask questions later." But security founded on the social contract must be baked into every aspect of IoT, from technology to policy and governance.

## Think Security Throughout the Entire IoT Lifecycle

IoT security can't be an afterthought. You can't just tack it on at the end and hope for the best. Security must be paramount in every aspect of the IoT lifecycle. For device manufacturers, this means integrating security into design, sourcing of materials, manufacturing, testing, deployment, and ongoing operations. For organizations that are providing IoT functions to customers or employees, this means that from the outset, security must be designed into every phase of standing up and operating your IoT systems. Start with security, then build your IoT products and systems around it.

And it's important to recognize, too, that IoT security doesn't end at the point of sale or the deployment. In fact, that's really just the beginning. Products and systems must be continually strengthened to fix vulnerabilities and protect against new threats. Thinking about this ahead of time – designing it in – can help you meet real-world security challenges. For example, how can you update your devices in ways that don't rely on the user to be proactive? This can be a tough problem – but you have to solve it now, not after all your sensors are out in the wild.



## Don't Leave Security to Chance: Make It Policy

Good intentions about IoT security aren't enough: You have to formalize them into clear policies that everyone will follow. For example, policies can make sure:

- That you consider the real cost. You can probably save money by building your IoT systems with less-than-secure parts and materials. But if you get hacked, the financial cost of reputational harm, lawsuits, or regulatory penalties could make you wish you had spent a little more upfront.
- That you buy hardware from manufacturers that can help your IoT systems scale. Too often, organizations buy products from sellers that can only produce a limited number, making it difficult for systems to grow.
- That your software and hardware aren't connected to your IoT systems unless they're secure. Some products are IoT ready, while others have no business being anywhere near the Internet. Policies can help make sure that you know the difference. In addition, policies that govern device connectivity can also reduce risk by limiting access when continuous connectivity is not needed.
- That you don't forget to incorporate fundamental cybersecurity practices. No matter how hard you work to protect your IoT, if you neglect basic cyber hygiene, your entire effort will be built on soft sand.

## Decide Now Who's Responsible for Security: Create a Governance Structure

Who is going to make sure the security policies are followed? How will the need for security be communicated to stakeholders? How much of the responsibility for IoT security should be centralized, and how much of it should be assigned to the individual business units? Without a governance structure in place, these kinds of questions are often dealt with on an inconsistent, ad hoc basis at first – and then later not at all. With well-thought-out governance, organizations can make sure that IoT security is aligned with business and mission goals – and the social contract.

Because the world of IoT changes so fast, both the policies and the governance structure need to be refreshed much more often than with traditional IT – generally every 6 to 9 months. If something needs to be changed earlier, don't wait. Set up a process for ongoing revisions.

## Create a Culture of IoT Security

IoT security isn't an IT problem – it's everyone's problem. That means it has to start at the top – including in the C-Suite – with a strong commitment and a clear direction. And it's up to leaders to make sure that commitment and direction cascades down to every level in the organization, strongly and clearly, and find their way into every corner.

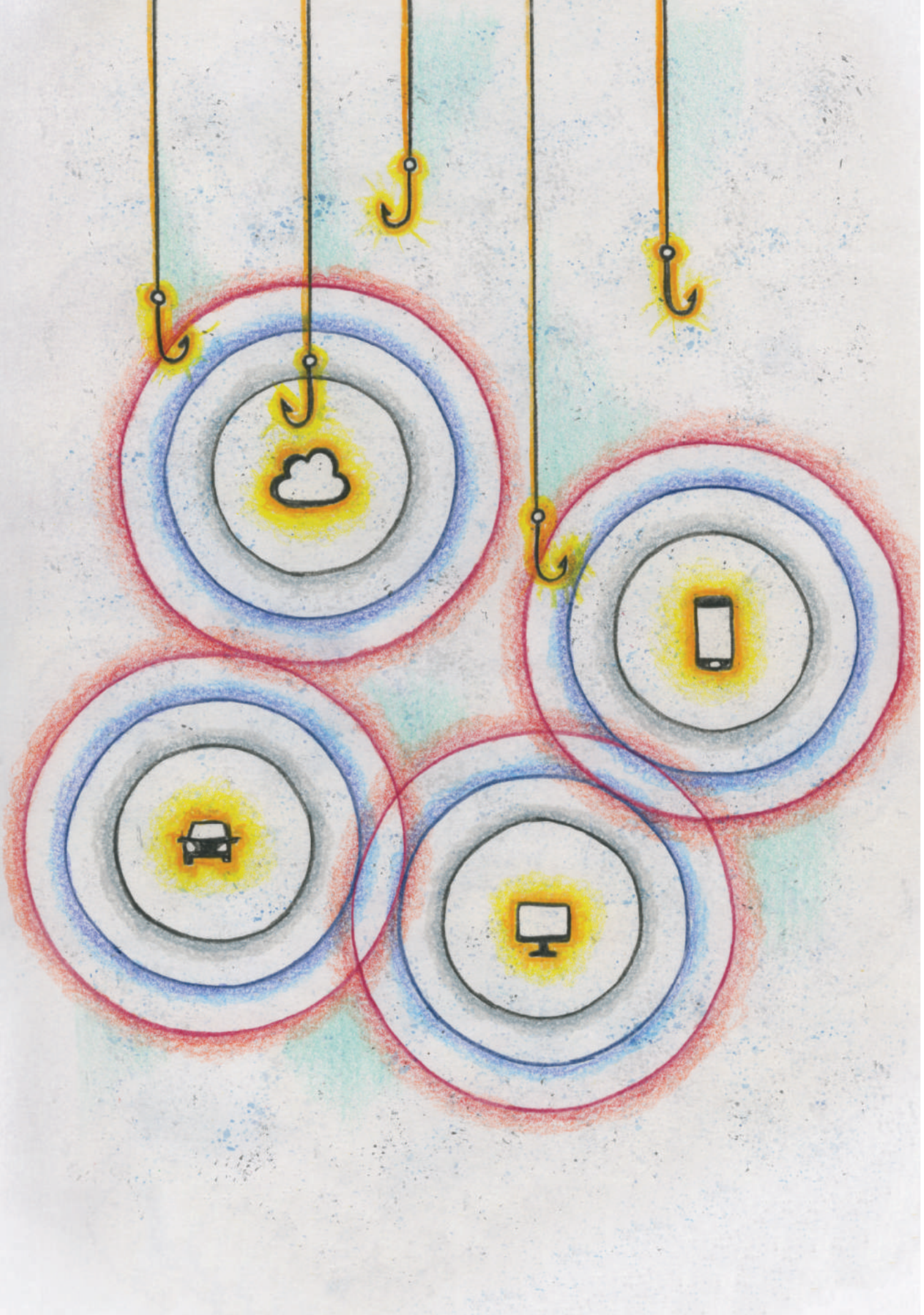
Leadership is just the start. If IoT security is to take root, it needs to be an integral part of the organizational culture. This extends from training and development to hiring and promotion, from research and development to marketing and finance.

And a culture of IoT security goes beyond organizations. No matter what your role is in the expanding IoT ecosystem – whether you're a provider or a user or both – IoT security is just as much your responsibility as anyone else's. If you leave it to someone else, you're the one who could lose out. But if you embrace IoT security – if you make it part of your IoT DNA – you can face the challenges ahead.



### Key Takeaways:

- No two IoT systems or architectures are alike – each requires a customized risk-assessment approach. And to keep pace with the changing threat landscape, risk assessments must be flexible and embedded in day-to-day IoT operations.
- Prioritizing resources is not a top-down exercise but an inclusive process that must involve stakeholders from across the organization. And once developed, the prioritization process should be regularly evaluated and updated.
- Advanced analytics can help spot hidden IoT attacks and build an evolving model of what healthy and unhealthy behavior looks like in your IoT systems.
- IoT incident response requires bringing together a wide range of stakeholders to develop a response plan, and then practicing it and refining it with scenario-driven exercises.
- IoT security will only take hold if it is "baked into" every phase of the IoT lifecycle and embedded into every aspect of the organizational culture.





# TEN ESSENTIAL PRINCIPLES **OF IOT SECURITY**

### 1. HONOR THE SOCIAL CONTRACT

How can you gain and keep the trust of your IoT users – whether consumers, employees, businesses, or government agencies?

### 2. UNDERSTAND HOW IOT IS MORE VULNERABLE THAN TRADITIONAL IT

How are your IoT system's edge devices, communication channels, and interconnections potentially opening the door for attackers?

### 3. IDENTIFY YOUR POTENTIAL ATTACKERS

Who is most likely to go after your data and devices, and why? How will they do it?

### 4. ASSESS YOUR RISK

What are all the ways your devices and data could be accessed and misused – and what would be the impact to your business?

### 5. PRIORITIZE YOUR RESOURCES

Given the risk of attacks, the potential implications, and your ability to fix vulnerabilities, where should you start? What's your long-term strategy?

### 6. BE PROACTIVE WITH THREAT DETECTION AND PREVENTION

How do you make sure you're going beyond mere compliance – which may not be enough? How can you build in resiliency so you can keep operating during an attack?

### 7. DON'T FORGET THE BASICS

Are you incorporating fundamental cybersecurity best practices? Are you connecting your systems deliberately? Are you reducing your risk by determining when continuous connectivity might not be essential?

### 8. "BAKE IN" IOT SECURITY

Are you making sure security is paramount in every phase of the IoT lifecycle, from design to supply chain to implementation and operations?

### 9. PREPARE FOR THE WORST

How ready are you to respond to a successful attack? Are you continually reassessing your strategy and your defenses?

### 10. DEVELOP A CULTURE OF IOT SECURITY

How can you instill a commitment to security in every corner of your organization? How can you achieve the necessary communication with stakeholders and provide users the right training?

# REAL-WORLD **EXAMPLES**

Putting IoT security to the test.

# DEVELOPING AN IOT STRATEGY FOR **THE OIL AND GAS INDUSTRY**

Nyla Beth Gawel

As private companies develop IoT capabilities, it's important for them to have a clear and coordinated strategy, with security as a top priority. The disparate nature of IoT often makes it harder for an organization to figure out where it should be focusing its investments and resources. Across many industries, a focus on efficiency and convenience has outweighed security in the early adoption. This fundamental problem was evident for an oil and gas company that had made ad hoc IoT investments but lacked a coordinated strategy to develop tools, knowledge, and processes to support the rollout of IoT systems. My team worked with the company to develop a consistent, scalable, and secure IoT strategy and architecture for use across the company.

Our goal was to develop materials and tools to focus their effort and investment moving forward. We performed the work with a systematic approach, focusing on an assessment of their current state of IoT guidance and policies as well as traditional IT policies and practices; developing an IoT reference architecture for the entire company; building out customized use-case architectures and examples; and finally, documenting a set of guiding principles for all layers of the technology stack for deployment of IoT systems.

Based on company input and discussions, we selected four high-value IoT use cases: connected worker, remote monitoring, predictive maintenance, and IoT services to customers/vendors. Applying Booz Allen's IoT Reference Architecture and IoT guiding principles to these use cases, our team prescribed future capabilities necessary to realize the business value of their IoT. With these use cases, we developed IoT Security Threat Assessment and Mitigation Guidance materials, which included a "Top 10" list of security questions that the company should ask itself and its vendors when setting up IoT systems. This list will help the company in thinking about critical factors, including vendor security.

## Top 10 Security Questions

1. Authority and Purpose
   Does the device support an industry or regulatory function?
2. Accountability, Audit and Risk Management
   What kind of security controls can the device support?
3. Security
   Does the device have security controls built in?
4. Monitoring and Enforcement
   What data will the device disseminate?
5. Management
   Are proprietary accesses needed for updates and maintenance?
6. Collection
   Where will the information be stored?
7. Access
   What are the physical links and controls?
8. Data Quality and Integrity
   What is the classification of the data and risks associated with it being transported?
9. Use Limitation
   Have security precautions been defined for the physical area?
10. Use, Retention, and Disposal
    What is the intended useful life of the device?

In the last phase of work, we developed a roadmap to prioritize investments across technology, organization, and governance categories to equip the company to invest in high-value IoT systems. Our focus on developing a clear and coordinated strategy, with security baked into every level, positioned the oil and gas company to make measured investment decisions about future IoT deployments.

# ANOMALY DETECTION AS A **SECURITY FRAMEWORK**

Steven Miller

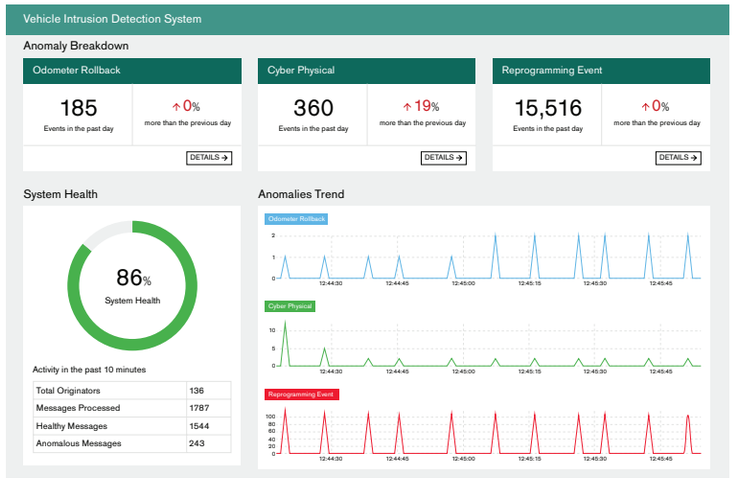
IoT cyber risk is inherently different than the safety, quality, and reliability challenges that product companies are accustomed to. There's an outside variable we can't control: cyber threat actors. That means we're not just engineering a solution: We're fighting an enemy. An adaptive, well-resourced, and highly motivated adversary.

To manage this new type of risk, organizations need to find the right tools that can help them stay one step ahead of the bad guys. One way to do this is to proactively identify and triage potential incidents using new data streams from connected products. But harnessing data for the cyber imperative can pose challenges: Talent is scarce, the scale and scope of data are unwieldy, and demonstrating value can be delayed by long-term development activities.

Working with an automaker, we set out to tackle these challenges, and show how to put data to work for the vehicle cyber mission. Within 6 weeks, we built a prototype anomaly-detection capability to allow vehicle cyber engineers and analysts to find and escalate potential issues faster. We chose data already available, to test solutions and get results quickly.

This approach required a collaborative effort among the product cyber, IT, and engineering teams. This can be a challenge for many IoT organizations. One key lesson learned is that partnering with other data-analysis efforts to share capabilities across business units is critical to early success. For example, Cyber and Safety efforts may be able to use similar data sets for different purposes. Frequent communication – articulating value propositions for all involved – is key, as is delivering quick wins.

We concentrated our efforts on gaining new insights by analyzing data that the electronic control units embedded in their vehicles had already generated and transmitted to a centralized repository via their telematics systems. These units are responsible for controlling everything from actuators in modern engines to the infotainment systems on a car's center console. The units are typically connected to the automaker's telematics back-end infrastructure to enable tasks like accident notification and remote diagnostics.




Example Dashboard for a Vehicle Health Profile

The data covered more than 100,000 vehicles. We had to ensure that we built an approach that didn't disrupt the business or cost more money while still providing meaningful insight. To achieve this, we built a highly scalable application that ingested vehicle data without creating a drain on computing resources. We also focused on making our application modular, to allow the team to refine and implement new rules over time that were indicators of cyber threats.

Once we integrated these data streams, we built an analytics engine and visualization tool to find insights and make them actionable. We developed a series of rules that could indicate a potential incident: Are things acting like they should? Where are the outliers? What are commonalities between vehicles with abnormal behaviors? These rules were analyzed individually and in the context of other rules to build a vehicle health profile that is constantly updated. And we calibrated alert thresholds for these rules over time to help sift through the noise by using clustering algorithms to build a model that defined normal, healthy behavior.

We knew that the value of analytics isn't in the numbers — it's in being able to apply them to business operations. So, we built an interactive visualization portal to provide vehicle cyber analysts real-time insights, with filter and deep-dive capabilities that allowed them to more fully analyze and understand the data. We integrated the analytic outputs into their operational model and processes. Using this tool as an input, the automaker is now better able to identify and assess potential incidents. By starting small, our capability showed value and got the necessary buy-in for more comprehensive, longer-term IoT security efforts to develop a full-scale solution that provides multiple analytics applications to reduce cyber risk.

# AUTOMATING SECURITY TO FIND **VULNERABILITIES IN MOBILE APPS**

Corey Garst

Mobile applications are increasingly becoming an essential component of IoT. That means finding vulnerabilities in mobile applications – before they're put into use – is more critical than ever. As with other IoT technologies, mobile app development often focuses primarily on adding capabilities and increasing efficiency, with security only as an afterthought.

Whether organizations deploy free public apps, buy them from vendors, or develop them on their own, they need to be sure that the apps are secure. While they've been relying more on automation, current automated processes have been limited – they typically can only find well-known, easy-to-spot vulnerabilities. People are still needed to do most of the analysis. That has become an increasing problem with the spread of mobile in IoT – many organizations are finding that they simply don't have the staff to do the much more extensive vetting for vulnerabilities needed. It's critical that automation take on a larger role.

Working with clients, we developed a capability that takes cybersecurity automation to a new level. In this case, we automated the process of identifying code vulnerabilities within mobile apps. This allows us to dissect the inner workings of the app and see how the key pieces fit together so that we can find larger risks in the application as a whole. It's essentially a form of reverse-engineering and is far faster than previous methods. With the automation, an analysis that might have taken a person days to complete can now be done within minutes.

This new capability doesn't entirely eliminate the human element: When vulnerabilities are found, people are still needed to understand how much of a threat they might pose to the organization, and to prioritize the necessary remediation. Ultimately, the capability frees up analysts for more higher-level analysis.

We believe that automating increasingly complex tasks will become critical to the success of IoT security. In essence, we're enabling the machines to do what they do best – automating repeatable processes. And we're enabling people to do what they do best – find insight in data and turn it into action.



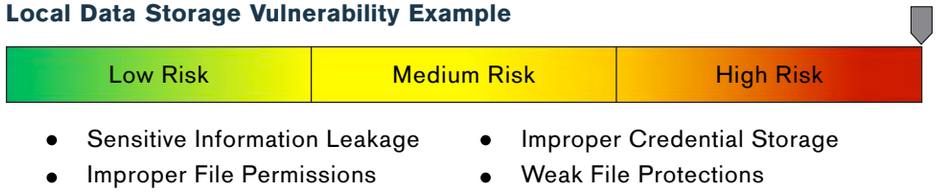
### Mobile App Security Risk Scale

Mobile Applications are assessed for risk within three categories, based on the findings such as those listed above.

**Code Vulnerability Example**

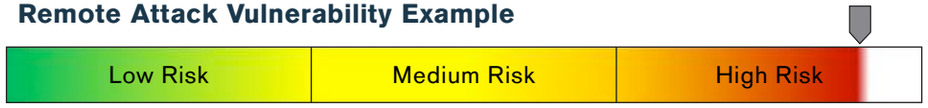

- Weak Cryptography
- Hard-Coded Credentials
- Unsafe Interprocess Communication
- Remote Code Execution

**Local Data Storage Vulnerability Example**




- Sensitive Information Leakage
- Improper File Permissions
- Improper Credential Storage
- Weak File Protections

**Remote Attack Vulnerability Example**




- Sensitive Information Leakage
- Personally Identifiable Information Disclosure to Ads/Analytics
- Man-in-the-Middle Vulnerabilities
- Improper Back-End Authentication

# DEPARTMENT OF TRANSPORTATION
# VEHICLE TWO-WAY RF SECURITY

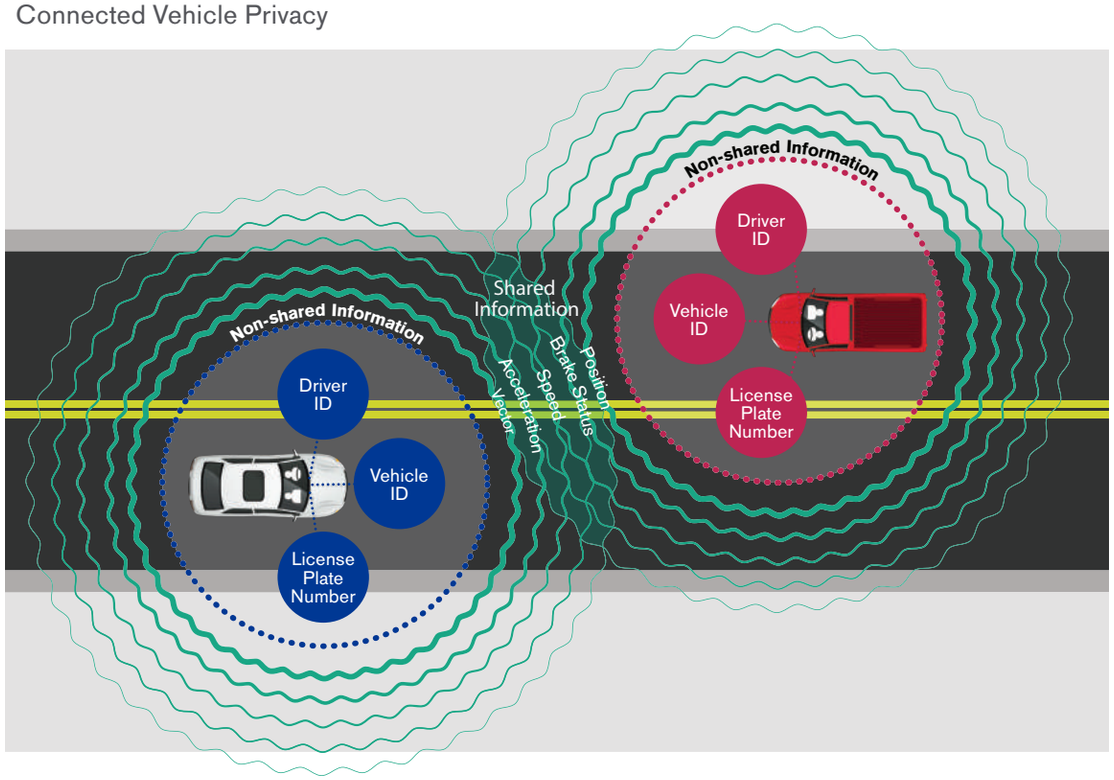
Dominie Garcia

The development of any IoT system requires an understanding of each layer and a serious effort to bake security into every level. The *edge* is the layer that really gives IoT its power, but it's also where traditional cybersecurity ways of thinking fall short. This new environment is filled with autonomously operating devices that communicate with each other and with more traditional infrastructure. In the area of connected vehicles, the need to understand vulnerabilities and ensure security could not be more important.

Our team worked with the U.S. Department of Transportation (USDOT) to better understand this new landscape. In the early 2000s, the Department of Transportation began to investigate the possibility of releasing new regulations and guidance around forth coming connected vehicle technology. Given the safety implications of vehicle-to-vehicle and vehicle-to-infrastructure technologies, the department was obligated to understand this new technology and its potential role in implementing and adopting it. *Dedicated Short Range Communications* (DSRC) is a two-way short to medium-range wireless communications protocol that permits very high data transmission critical in communications-based active safety applications. As part of USDOT's consideration of regulating or mandating this technology in passenger vehicles, it needed to be assured of user security and privacy.

We worked with the department to evaluate the technical design of the security system being developed by a pre-competitive automobile manufacturer consortium (the Crash Avoidance Metrics Partnership). The consortium developed a modified public key infrastructure design to ensure the security and privacy of vehicles with DSRC capabilities. In conjunction with the consortium, we supported development of cost models, organizational designs, and institutional or governance models for this security system.

Connected Vehicle Privacy




While other networks and communication methods for connected vehicles are seeing significant cyber threats, and the industry is catching up in terms of how to protect vehicles and data, DSRC's implementation nationally will be conducted with a built-in set of protections. These protections are the result of a thorough understanding of the technology's vulnerabilities and security that is baked in by design.

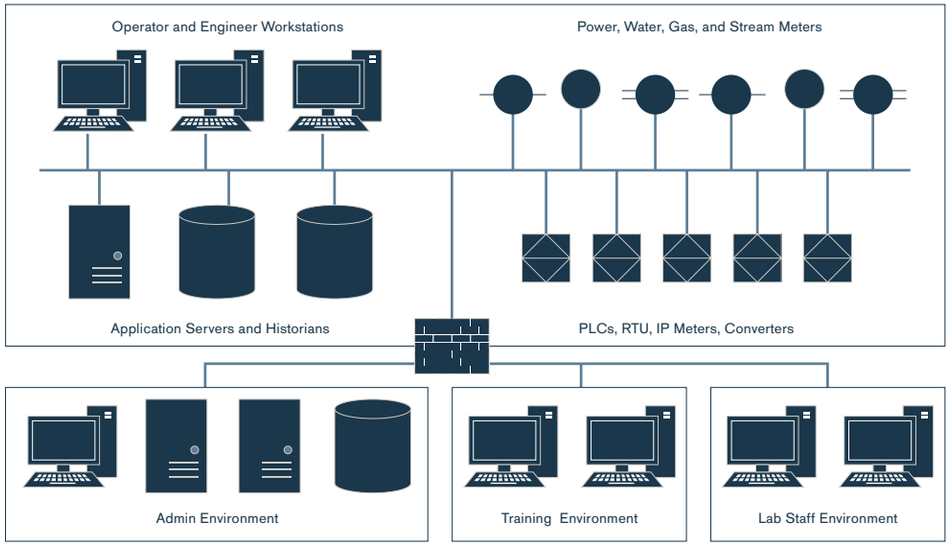
# DESIGNING AN **INDUSTRIAL IOT TESTBED**

Caitlin Ferro

Modern industrial and manufacturing processes rely on a vast array of Industrial IoT devices – telematics and smart devices that support automation and provide data essential to day-to-day operations. But until recently, industrial control systems (ICS) were designed with an emphasis on reliability and safety without much consideration for cybersecurity. With the introduction of more sophisticated and interconnected industrial IoT devices, however, ICS processes are open to new vulnerabilities, creating the potential for attackers to penetrate, disrupt, and damage operations.

This makes it increasingly necessary to evaluate all proposed changes to ensure that existing reliability and safety margins are met and that cybersecurity measures can be deployed without impeding operations.  As an example, patches – whether designed to remedy security vulnerabilities or to improve performance – could potentially affect control system interactions, maintenance operations, and training. Therefore, changes to industrial IoT devices and software, such as smart meters and process applications, must be made and tested in a controlled manner.

During an engagement with a large facilities management organization, my team developed a design and rollout plan for an industrial IoT testbed. There were several goals for the testbed, including testing new control systems and devices before they were deployed and supporting control systems software application development and baseline testing. The testbed also allowed us to evaluate how existing control systems might respond to cyberattacks. We were able to incorporate the organization's most commonly deployed devices and software applications so that many different types of use cases could be modeled.




High-Level Testbed Design

The testbed also served as an educational tool. With the rollout of new ICS processes, successful implementation requires a strategy to communicate changes and train your users. Proper training is vital to an organization's operational and security practices when new technology is introduced. As such, the testbed can be a tool in the overall IoT security strategy used to educate both IT and control systems operations personnel who monitor, control, and perform system and network administration for building control and utility control systems.

Ultimately, the testbed and rollout plan were incorporated into the organization's broader IoT security strategy. The plan included design diagrams and network topology diagrams to map out the specific IT and operational technology hardware and software. It also included human–machine interface simulation software for the testbed and training classrooms. These measures, enabled by the testbed, provided the organization with a formal process for ensuring that its current and future industrial IoT devices and software applications are deployed securely.

# AUTOMOTIVE CYBER **INCIDENT RESPONSE**

Alexandra Heckler

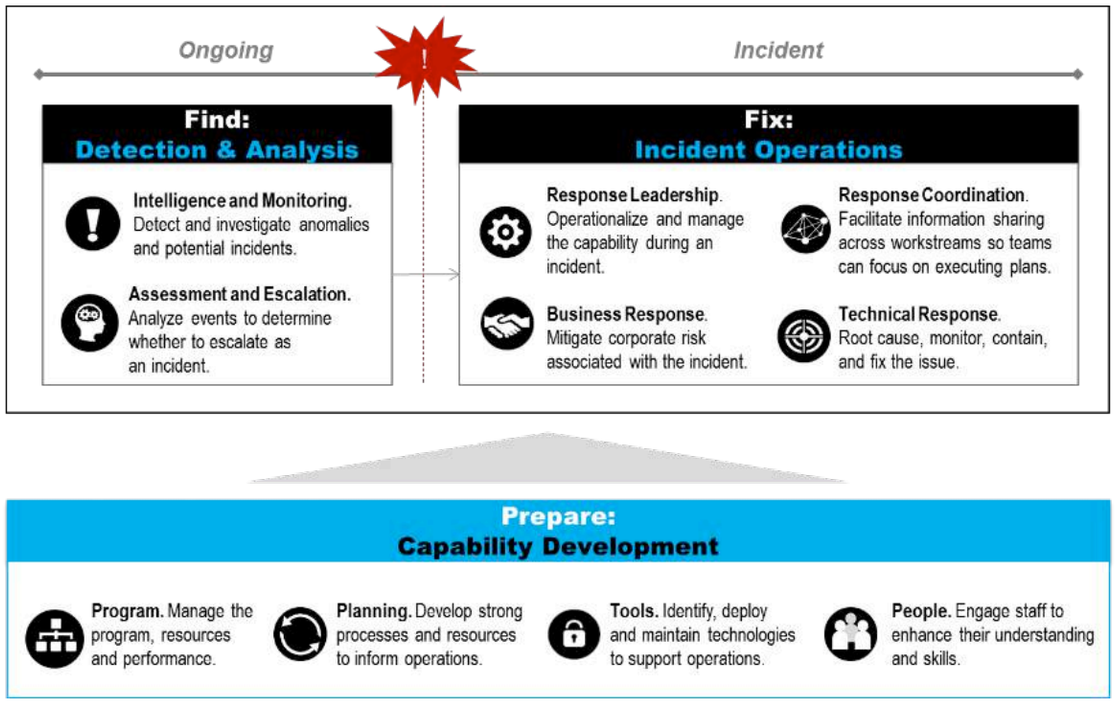
Months before the infamous Jeep hack was featured on the front page of *Wired Magazine* in July 2015, one automaker already had a plan in place to respond to real-world vehicle cyber incidents. In 2014, this automaker partnered with our team to prepare for vehicle cyber incidents.

At the time, there was no common definition of a vehicle cyber incident, no playbook for response, no standards, and no experts. But we knew that product cyber incidents are different than traditional enterprise IT incidents. Product cyber incidents can potentially affect customer safety and privacy. They affect the brand. They can originate within your firewalls but also "out in the wild." They require a coordinated, organization-wide response that brings together all corners of the business to address corporate and technical risk.

We quickly learned that vehicle cyber incident response was as much about culture as it was about documenting a plan. Even setting a common definition for a vehicle cyber incident was harder than expected. It overlapped with safety, privacy, IT, quality, and many other business areas. But we knew a clear definition and a single, accountable leader would be critical to effectively coordinating a whole-of-business response. So, we took it slow, we socialized our work and progress, and we kept revisiting our solution until we got it right. We engaged stakeholders throughout the development of critical resources to make sure they knew what a product cyber incident looked like, what their role was, and why it mattered to the business.

Together with representatives from across the automaker, we developed a comprehensive set of tools and capabilities, including:

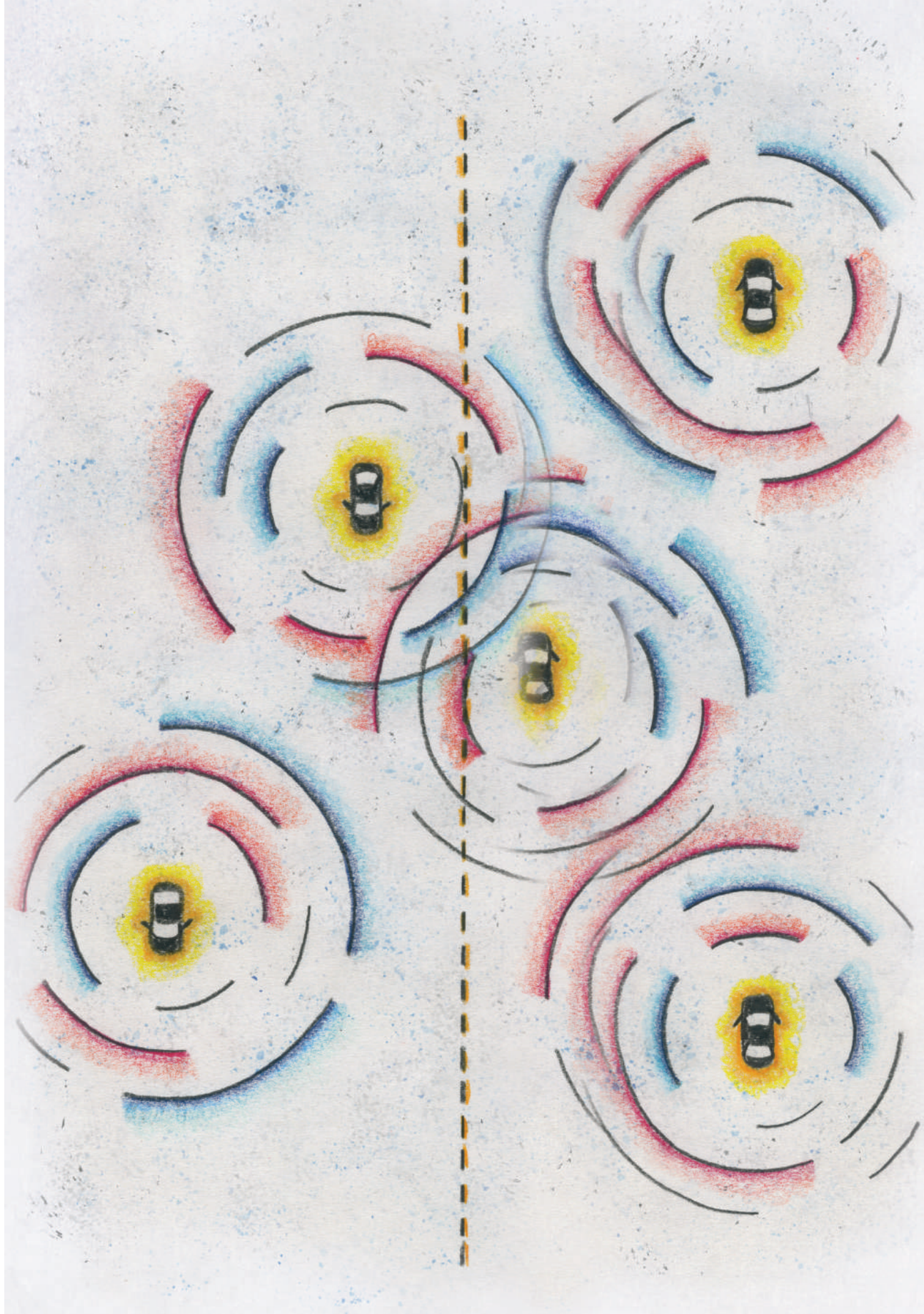
- **Incident Response Framework.** Captures high-level process steps, decision authorities, and call sheets in a "placemat format" to provide a quick-start guide when crisis mode hits
- **Incident Response Plan.** Defines and documents a detailed approach to incident response, including roles and responsibilities, decision authority, and process steps, to coordinate a consistent, complete response
- **Playbooks.** Provide role-specific checklists, resources, and success criteria to guide response activities
- **Severity Matrix.** Creates a common language for incident severity and sets corresponding standards for response. (e.g., timeframes, frequency of updates, level of decision authority)
- **Containment Options Chart.** Documents options to stop the bleed, including key considerations and decision authorities, so they can rapidly be deployed when a crisis hits

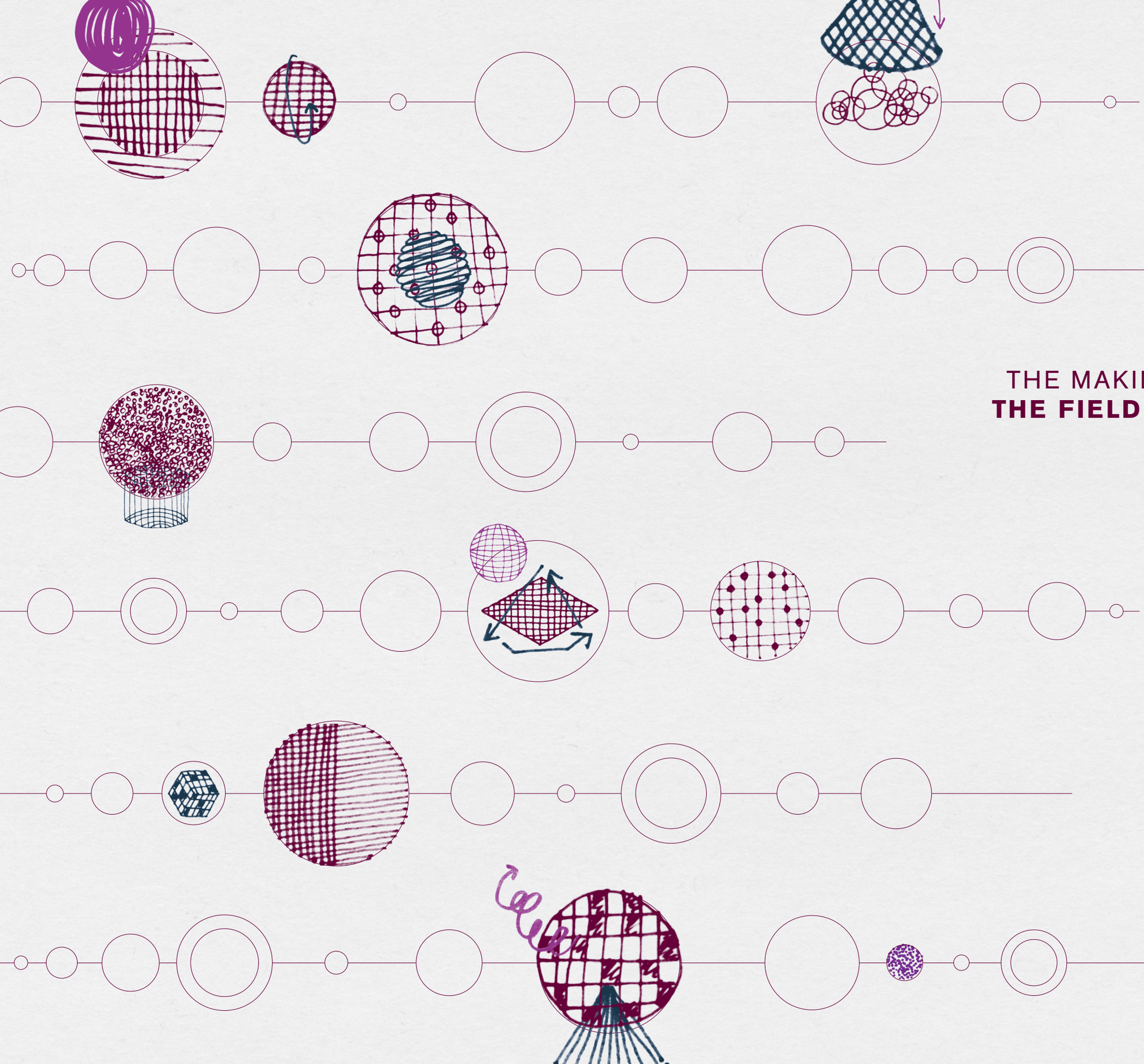



Elements of a Mature Incident Response Capability

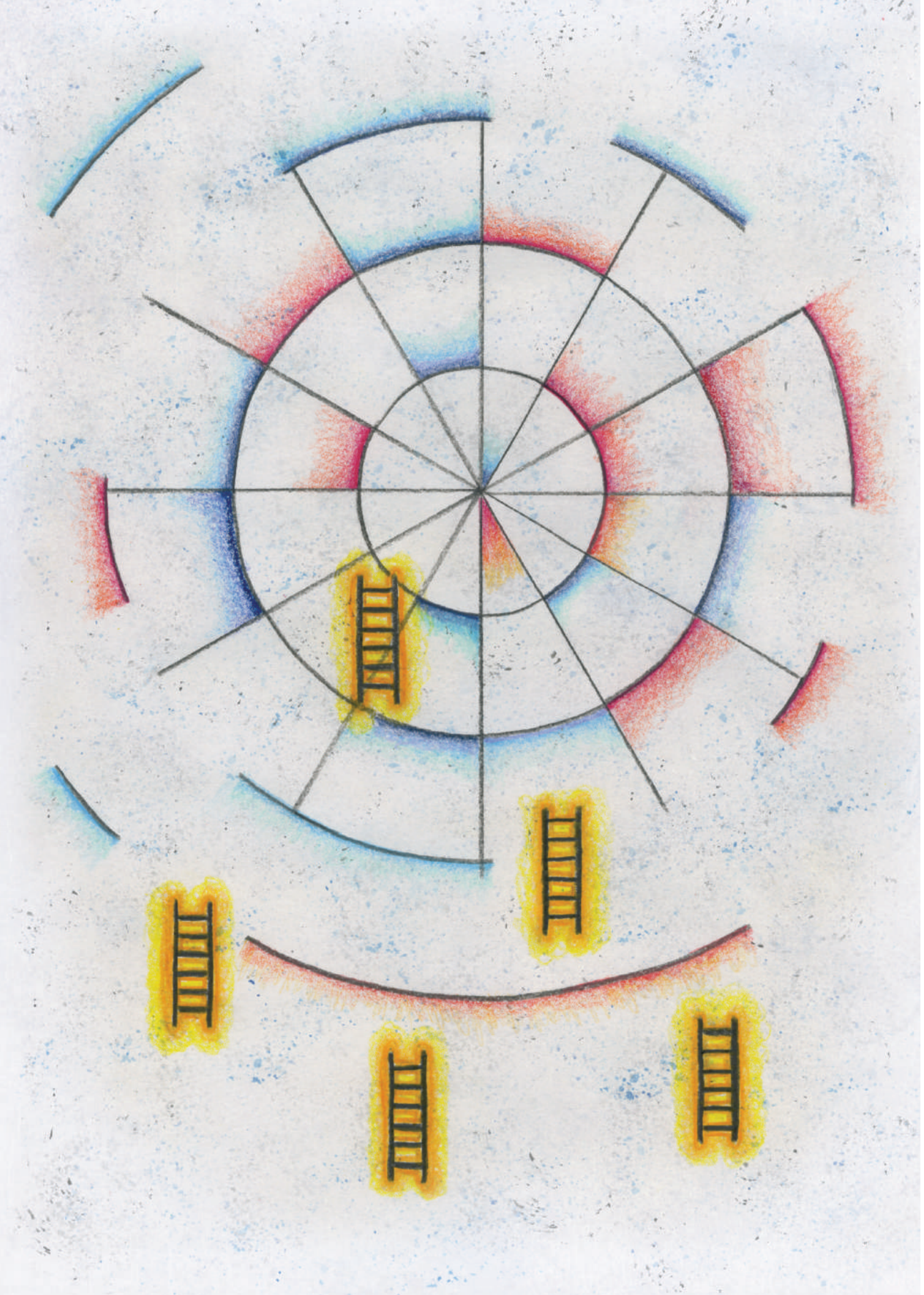
The next step was to practice using the plan. Our first exercise focused on orientation: what the challenge was, why it mattered to the business, and how the team's roles were relevant. Participants challenged us to articulate why they were in the room. The second exercise was a stark contrast to the first: People were on board, knew their role, and were ready to jump in. Not only that, but the team grew — from 30 to 45 people — because people understood the breadth of roles and organizations that needed representation, and wanted in.

The result was a first-in-the-industry capability: the tools, resources, talent, and awareness to respond to vehicle cyber incidents. This capability is now directly informing best practices across the industry. The effort shifted the company culture, prioritizing product cybersecurity, and the automaker has the confidence to tackle vehicle cyber incidents while minimizing the impact to customer safety and privacy.





# THE MAKING OF
# **THE FIELD GUIDE**





# PARTING **THOUGHTS**

Until recently, discussions about IoT security have been like distant thunder: we know a storm is coming, but there's no real urgency to seek shelter. Now, though, the storm is getting closer – the growing number of news stories about IoT hacks are like the first wave of raindrops splotching the sidewalks and streets. Everyone is taking IoT security more seriously than ever, and with good reason.

We hope that with this field guide, we've given you some insights to help weather the storm. Many of those insights have come from our work with clients across business and government. We thank them, and we thank you for taking this journey with us. We believe that the future of IoT is bright, and that, with sensible approaches to security, its promise will be fulfilled. Let's make it happen.

# AUTHORS

**J. Bradley Medairy**
*Senior Vice President*

**Eric Rickard**
*Vice President*

**Andy Linn**
*Principal*

**Nyla Beth Gawel**
*Principal*

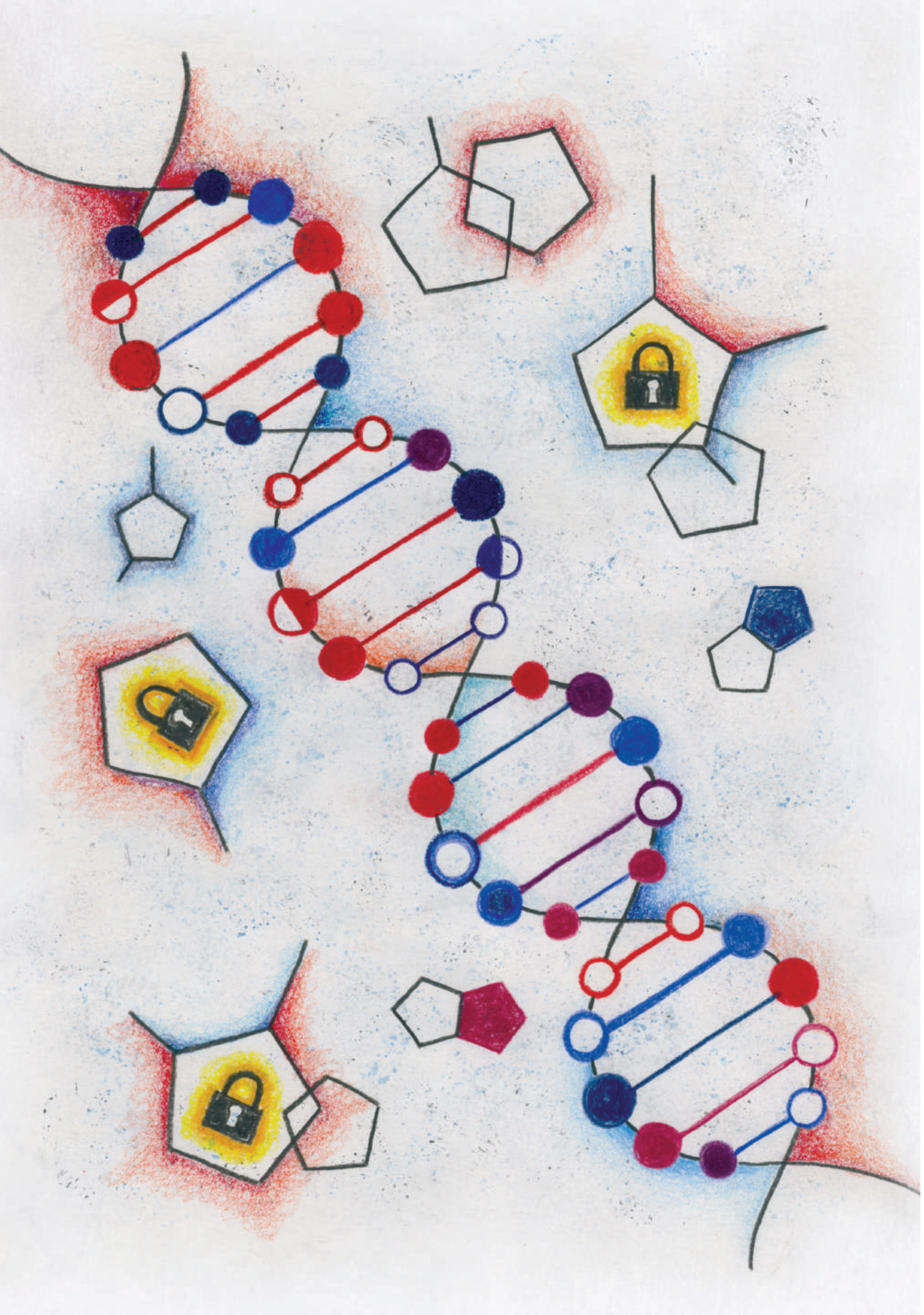
**Mike Delurey**
*Principal*



# ACKNOWLEDGEMENTS

This field guide would not have been possible without generous contributions from the following Booz Allen Hamilton staff:

Jamil Albertelli
Brandon Ayers
Nathaniel Beach-Westmoreland
Jaco Botes
Denis Cosgrove
Patrick Duma
Jason Eller
Will Farrell
Scott Flander
Caitlin Ferro
Dominie Garcia
Corey Garst
Doug Gartner
Doug Hamrick
Anthony Harris
Alexandra Heckler
Steven Miller
Steve Mills
Scott Stables
Jacob Styczynski





# ABOUT **BOOZ ALLEN HAMILTON**

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years and embraces the core consulting values penned by our founding partner, Edwin Booz:

- Start with character, intelligence, and industry.
- Daily – think right, act right, eat right, sleep right, work right, and play right.
- Know your own blind spots.
- Always be willing to listen and to help worthy young people.
- Require character, intelligence, and "hard work" as the starting foundation in selecting people.
- Pick the cream of the crop for your partners.
- Fear not the future, nor people.

Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and nonprofit organizations across the globe. Booz Allen partners with public and private-sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs more than 22,500 people globally and had revenue of $5.4 billion for the 12 months ending in March 31, 2016. To learn more, visit www.boozallen.com. (NYSE: BAH)

# REFERENCES


1. Mlot, Stephanie. “HVAC Vendor Confirms Link to Target Data Breach.” 7 February 2014. *PCMag*. <http://www.pcmag.com/article2/0,2817,2430505,00.asp>.

2. Perlroth, Nicole. “Hackers Used New Weapons to Disrupt Major Websites Across U.S.” 21 October 2016. *The New York Times.* <http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=1>.

3. Booz Allen Hamilton. “When the Lights Went Out.” 2016. *Booz Allen Hamilton.* <www.boozallen.com/ics>.

4. Bennett, Cory. “FBI Chief: Terrorists Plotting Cyberattacks Against the United States.” 23 July 2015. *The Hill.* <http://thehill.com/policy/cybersecurity/248930-fbi-head-terrorist-groups-plotting-cyberattacks-on-us>.

5. Tucker, Patrick. “How Will Terrorists Use the Internet of Things? The Justice Department Is Trying to Figure That Out.” 8 September 2016. *Defense One.* <http://www.defenseone.com/technology/2016/09/how-will-terrorists-use-internet-things-justice-department-trying-figure-out/131381/>.

6. Santora, Marc. “In Hours, Thieves Took $45 Million in A.T.M. Scheme.” 9 May 2013. *The New York Times*. <http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html>.