CIO DECISIONS

Guiding technology decision makers in the enterprise

JULY 2016 VOLUME 54

The Trek to Blockchain

The technology behind bitcoin holds promise for changing how business gets done. But the path to implementation isn't easy—and companies will need to follow a detailed map to get there.

TechTarget

Francesca Sales
Site Editor

It's Time to Get Enlightened About Blockchain

BLOCKCHAIN, THE PEER-TO-PEER distributed ledger used to validate transactions, thus creating an immutable record, is getting a lot of buzz from observers of the technology, particularly for promising potential blockchain use cases in industries like financial and legal services. One such proponent, Bill Caraher, of law firm von Briesen & Roper, puts the "sweeping implications" of blockchain this way:

Deploying blockchain could determine "the authority of documents and [prove] their originality, their state, their disposition, their destruction and just be the index of the real story," the CIO and director of operations told Sue Troy in the cover story of this month's *CIO Decisions*. It could also "lead to speedier resolutions ... better evidence gathering [and establishing] foundation for a case," he said.

Caraher isn't alone in his enthusiasm over the technology and its implications; technology vendors active in this space, such as IBM and Microsoft, told Troy that they're receiving inquiries into blockchain from industries outside of finance and legal services, including utilities, advertising, healthcare, auditing and real estate. Indeed, while the financial services industry has won the status of early adopter because of its early awareness of Bitcoin, experts say that blockchain will benefit many other industries. But there is one thing still missing that is keeping this and other potential use cases from taking off, and that's the full development and productization of blockchain, writes Troy.

Blockchain implementation all starts with Stage 1: sorting through possible blockchain use cases and scoping out a technology plan for them, a process that is more difficult than it seems, and probably the most important.

"The most pragmatic question [for IT to ask about blockchain] is, To what products does blockchain apply; but more pragmatically, how does blockchain not apply?" Jeff Garzik, co-founder of blockchain services and software company Bloq and a core bitcoin developer, told Troy.

Flip through our cover feature to learn about how to pinpoint potential blockchain use cases and the critical steps to putting them into action. Plus, we answer technical questions and home in on the consumer use case.

Please write to me at fsales@techtarget.com.

The Trek to Blockchain

To realize the potential of blockchain, get ready for a lengthy process.

BY SUE TROY

ART: MARABELO/FOTOLIA

BILL CARAHER ENVISIONS the day when blockchain technology will "substantiate and with zero doubt prove" the origins of documents and contracts used in the legal industry. For Caraher, CIO and director of operations at von Briesen & Roper, a 250-employee law firm in Wisconsin, this capability would be monumental.

Blockchain technology—in which a peer-to-peer distributed network is used to validate transactions and other records, which thereby creates an immutable record—will have "sweeping implications" around the provenance and authenticity—or lack thereof—of legal documents

and agreements, he said.

A blockchain implementation could determine "the authority of documents and [prove] their originality, their state, their disposition, their destruction and just be the index of the real story," Caraher said. "It could lead to speedier resolutions; it could lead to better evidence gathering [and establishing] foundation for a case."

Caraher eagerly anticipates the development of technology that would help make that potential a reality. But like many of the potential use cases for blockchain technology, the one Caraher foresees hasn't yet been fully developed or productized.

Indeed, potential use cases are a favorite topic among blockchain observers, and it seems that every conversation about the technology yields a new one. But sorting through which blockchain use cases actually make sense takes some work. And then having software—and in some cases hardware, for IoT-enabled scenarios—to put that use case into action is another step. But companies will eventually get there, proponents say, through concerted and judicious efforts among CIOs, IT practitioners, IT vendors and developers alike.

BILL CARAHER, *CIO, believes blockchain will have an impact on legal services.*

IMPACT ACROSS VERTICAL INDUSTRIES

IT's involvement with blockchain implementations—and therefore the level of urgency associated with putting this technology into operation—will to some degree depend on the vertical industry the company is in, with financial services being the most urgent. But as evidenced by Caraher's enthusiasm for blockchain's application to legal services, interest in the technology is widespread.

Vendors active around blockchain—both broad IT vendors such as Microsoft and IBM as well as niche blockchain suppliers—say they're fielding calls from virtually all industries. Beyond financial services and legal, others include: insurance, utilities, public sector, advertising, healthcare, auditing, supply chain, manufacturing and real estate, to cite some that have been mentioned.

Banks are under particular pressure to get going on blockchain implementations because they're facing pressure on three fronts, said Jeff Garzik, co-founder of blockchain services and software company Bloq and a core bitcoin developer: Technology companies like Apple and Google are rolling out payment software; telecom companies are enabling consumers to use their mobile phones as a bank account, to pay bills and send money; and cryptocurrencies such as blockchain-based bitcoin and Ethereum are being used to disrupt banks much the same way tech and telecom

(Continued on page 6)

Tech Questions: Scalability, Consensus, Data Ownership

WE ADDRESSED QUESTIONS around the scalability of blockchain systems, how consensus works and ownership of the data to Arvind Krishna, senior vice president and director of research at IBM. The company is aiming its efforts in the permissioned blockchain space, in which there are no anonymous players.

Scalability. Krishna said that in the permissioned (and non-cryptocurrency) blockchain system that IBM envisions, scalability—which can be a problem in permissionless systems—isn't a concern for three main reasons. In a cryptocurrency blockchain system, like bitcoin or Ethereum, scalability is limited by the number of transactions per second, the size of the network and the number of coins. Some estimates say bitcoin can currently support seven transactions per second, compared with anywhere from 1,000 to 2,000 per second by Visa, depending on whose estimates you use. In a non-cryptocurrency blockchain system, those limiting factors fall away, he said.

Consensus. How many peer-to-peer nodes is enough for consensus is determined by Byzantine fault tolerance theory: A certain percentage of actors in a system can act maliciously or in collusion with one another without compromising the system's validity. A blockchain system designer can avoid collusion by, for instance, requiring geographical representation among peers on the network.

Bitcoin has about 5,700 nodes in its network as of early June. In permissioned blockchain, the network can be much smaller. "If it is a small network, you might ask for consensus by all nodes agreeing," Krishna said.

Data ownership. In a public blockchain system, all the nodes on the network are responsible for holding the data. If one or more of those computers goes down, "as long as a sufficient number of the nodes in the network are there, you preserve the whole property" so that the system remains viable, Krishna said. He envisions some kind of administrator—suggesting IBM will offer this as a service—that would handle backup chores and provide audit logs. ■

(Continued from page 4)

companies are. But, he said, the disintermediation to banks will not be all-encompassing. "You're not going to have Aunt Joan and Uncle Joe store all of their wealth on their smartphone, for example. Banks are still going to exist and provide loans and provide services that strictly cash-like bitcoin and Ethereum systems do not provide."

Yorke Rhodes, global business strategist at Microsoft, said that the financial services industry got a head start on developing uses for blockchain technology because it had early awareness of bitcoin. "It's pretty easy for people to be able to pivot and say, 'Well, we understand bitcoin and the underlying technology. What else can we do with this? And, oh, by the way, this may be more disruptive to our business than bitcoin, because bitcoin is really just a payment vehicle.'" Despite the first-mover status of the financial services industry, many other industries will benefit from the technology, Rhodes said.

GETTING STARTED ON BLOCKCHAIN

Garzik identified four stages to a blockchain implementation, and they apply no matter the industry a company is in. In Stage 1, a use case is identified and a technology plan is scoped out. Stage 2 is a proof of concept. Stage 3 is a field trial, which involves a limited-production run with customer-facing data, which is stepped up to involve more customer-facing products and data volumes, he said. And Stage 4 is a full-volume rollout in production. Almost no organizations have reached Stage 4, Garzik said.

> **"Banks are still going to exist and provide loans and provide services that strictly cash-like bitcoin and Ethereum systems do not provide."**
>
> —JEFF GARZIK, *co-founder, Bloq*

When it comes to Stage 1, "the most pragmatic question [for IT to ask about blockchain] is, To what products does blockchain apply, but more pragmatically, how does blockchain not apply?" said Garzik. "Some of the systems that are being converted are being explored more out of interest rather than being directly driven by customer value. So what areas of blockchain deliver the most customer value? That's the key question that CIOs should be asking."

Joe Guastella, global leader of Deloitte Consulting's financial services practice, said that some clients are approaching the firm with a clear idea that they want to understand how blockchain might be used, whereas others come

to the firm with a business problem, with no preconception that blockchain should be used. "There are people who are saying, 'We have these problems. ... We've got to take costs out.' And we kind of shape out and scope out the problem statement. And then you look at what the solutions may be.

It's important for companies to gain expertise in-house because blockchain is both new and complex.

And then you have some that say, 'You know what? This may lend itself to a blockchain solution because it'll cut out these 10 post-transaction reconciliation steps, and therefore you can save this much money.' "

Regardless of how the use case is discovered, companies that have identified a use case will either look to their vendor partners for a product that fits the bill, or will work to develop the technology internally.

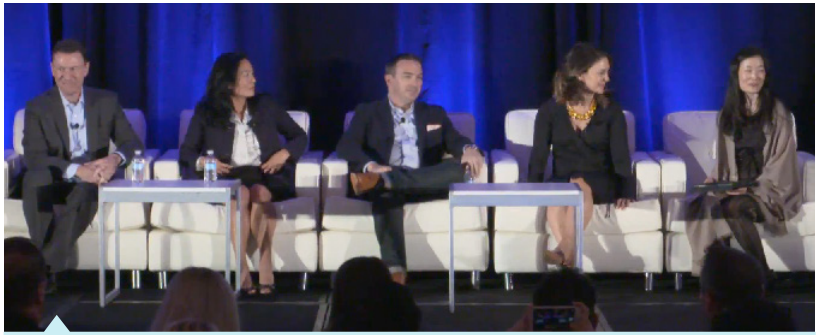
Smaller companies are more likely to look to a vendor to supply a product. "I would see us working with one of our existing vendors to say, 'Are you forming an advisory panel or exploratory group of existing law firm clients that would want to roundtable about this and how do we see it as a benefit to the firm?'" Caraher said. He said that von Briesen & Roper would most likely work with its niche vendors in the document management space to see how they could incorporate blockchain technology into their products. Use of products employing blockchain technology would be a competitive advantage for his firm, Caraher said.

For larger companies, once a use case has been identified, Rhodes said, the next step is to identify an architecture to address the use case. And as with all IT projects, IT will need to determine a budget, a deadline and whether the work can be taken on using internal resources or whether outside help is needed. He said most companies will choose to contract for outside help with blockchain. "It's going to be way too hard to get up to speed in a sensible way across multiple complex technologies that are three or four different potential competing variants," he said.

Garzik, however, noted that whether doing a blockchain implementation internally or with outside help, it's important for companies to gain expertise in-house with blockchain technology because the technology is both new and complex.

For IT shops looking for help with a blockchain project, there's a very broad if still-immature ecosystem developing around the technology. According to a recent report from 451 Research, there are almost 300 bitcoin- and blockchain-related startups across the globe, operating to develop tech-

nology in the financial, productivity, storage, smart contracts, social networking, supply chain management, identity management, governance, retail and IoT product spaces. Most big IT vendors are active around blockchain, notably IBM, which has put considerable resources behind the Linux Foundation's Hyperledger Project, and Microsoft, which is working with banking industry consortium R3 CEV to enable testing of blockchain systems using Microsoft Azure. And the large consultancies and systems integrators have also developed practices around the technology.



Blockchain panel members at the Consensus 2016 event, from left: Eric Piscini, Catheryne Nicholson, Scott Mullins, Meltem Demirors and moderator Laura Shin.

PROOF OF CONCEPT

Garzik described the proof-of-concept stage as a one- to three-month exercise. "You create a system ... that integrates into an isolated sandbox environment with that ... institution's data and you get to see the software operate in a simulated environment with real customer data. It does not impact customers but it's real customer data, real transaction volume," he said. "If you're talking larger volumes, a million transactions per day—something of that nature—you get to see how well the blockchain system scales up to meet that demand."

At the Consensus 2016 industry event in May, Catheryne Nicholson, CEO and co-founder of BlockCypher Inc., which builds blockchain APIs, explained the proof-of-concept process in a panel discussion. "[A proof of concept is] very un-methodological in terms of engineering; it's something where you're trying to iterate quickly, fail quickly. It's the mantra of 10 engineers doing 10 projects in two months and seeing what's sticky."

Both BlockCypher's Nicholson and Microsoft's Rhodes said the cloud is the best venue for a proof of concept. "[Cloud computing] lets you spin stuff up without worrying about hardware [or] about it being inside your network," Rhodes said. Having it in the cloud also makes sense if there are multiple organizations participating in the proof of concept, he added.

(Continued on page 10)

Blockchain and the Consumer Use Case

MICROSOFT HAS BEEN working closely with its large enterprise customers to help them map out blockchain strategies. But, as you might expect, the company is not ignoring blockchain in the consumer space.

As an example of how Microsoft is interested is watching blockchain for consumers, Yorke Rhodes, global business strategist at Microsoft, pointed to a company called Slock.it, which sells technology to control physical objects, such as locks, linked to smart contracts that run on the Ethereum blockchain.

"You can use blockchain to provide secure ways to share stuff that doesn't necessarily involve an Uber or an Airbnb or a sharing economy company," Rhodes said. "Slock.it also has a consumer IoT hub. … It's basically a little computer that sits on the blockchain that's also an IoT hub to connect other IoT devices in homes."

Rhodes also pointed to the idea of charging electric vehicles at places other than today's dedicated charging stations. One of the gating factors in the sale of electric vehicles relates to the infrastructure around charging the vehicles: Long trips away from an owner's home base are highly dependent on the location of existing charging stations.

Rhodes explained: "There's electricity everywhere. The question is, How do you charge for it? If you can figure out a way so you can securely identify a consumer that's going to charge from a distributed electrical outlet that might be on the side of someone's building or someone's house or garage or gas station or whatever and be able to distribute the fees associated with that appropriately, and do it securely and make it all seamless to the consumer, you've started to create a much more significant charging infrastructure for electric vehicles."

Rhodes suggested that Microsoft may choose to embed blockchain technology into the operating system. "We could say, 'Hey, we have a great operating system adopted by tens and tens of millions of people. What if there is technology that we could build into the operating system and/or in the browser that would help Joe Consumer be on the blockchain by default?'" ■

(Continued from page 8)

Even though testing may be done using public cloud services, most companies will relegate those tests to private or permissioned blockchains. "No enterprise is going to do the first tests on the public blockchain, so I think you'll see a ton of use cases in development that are 100% internal only," Rhodes said.

There are obstacles that will derail a proof of concept. At the Consensus 2016 event, Scott Mullins, who runs worldwide financial services business development for AWS, implored IT organizations to include all relevant parties in a proof of concept. "Don't forget you've got people down the chain that you need to include in the [POC] process. You've probably got a third-party outsourcing team, you've probably got a third-party oversight team, you've definitely got a compliance or risk management team," he said. "Don't wait to get all the way to the end with your POC ... and you have five people who raise their hands and say, 'Hey, you need to talk to us about the different things we need to check the boxes on.'"

Eric Piscini, consulting principal for Deloitte's Technology and Banking practice, speaking on the same panel, advised against a wide-scale POC. "When we see POCs fail, most likely you start too big and think you're going to change the whole organization with blockchain. My advice: Start with something small that's going to impact a very small part of your organization."

Nicholson cautioned against lengthy contracts tied to a proof of concept. "From a startup perspective, we have been thrown 150-page boilerplate master services agreement for a POC. It's way overkill. If you're an institution looking to do a POC, put that MSA to the side. Ask the startup if they will work with your four- to five-page agreement instead of going through months and months of negotiation with legal counsel, before you even start."

FIELD TRIAL AND BEYOND

After proof of concept comes the task of putting real data into production.

Garzik said this typically means a small trial with perhaps 5% of customers or customers on a lower-volume product. "IT staffs are locating within their customer product sets perhaps a lower-volume, perhaps less-customer-facing, use case that they can then present both to the board at the CEO level and also to their engineers at the low level to really gain that knowledge."

Nicholson explained that the field trial isn't simply a proof of concept moved to production but rather a restart. A field trial might have completely different requirements than a POC, she said.

Rhodes noted that once businesses become comfortable

with the software they're using and are happy with the testing process, they may choose to implement blockchain projects on on-premises hardware within the enterprise rather than in the cloud.

Nasdaq's Linq system, which uses blockchain technology to manage private-market trades and which went live on Dec. 31, is an example of a blockchain implementation at Stage 3, Garzik said. "That's a field trial with real customers. But it's not as high-volume as turning the Nasdaq tech stocks on the blockchain. The number of trades for Microsoft or Apple stock is easily 10,000 times the number of trades on [a system like Linq]."

"Most customers are not yet at Stage 4," Garzik said. "Fortune 500 is really at Stage 2 POC or Stage 3 field trials with blockchain technology."

A full-scale production system requires a much greater commitment to the blockchain application than the prior stages. "Production is out in the wild, where it has to scale, all the users have to be happy, you have to have help desk. Essentially it begins to run on its own," Nicholson said.

And achieving that stage has so far eluded most blockchain projects.

"The only POC that's in production is bitcoin. It's the only blockchain that is out in the wild, that has come under attack, that's stood the test of time," said BlockCypher's Nicholson. "Everything else is a bright shiny baby and is theoretical." ■

Shawn Wiora
CIO
Creative Solutions in Healthcare

Cloud Unites IT with Patient Care

THE PROBLEM: The IT situation at Creative Solutions in Healthcare was pretty dire two and a half years ago. When CIO Shawn Wiora came on board, he found alarming security issues. The company's outdated Windows Server 2003 machines were out of sync with current security protocols. Patch management as a formal program was practically nonexistent. There was very little documentation of HIPAA compliance. "From a security perspective, it was a ticking time bomb," Wiora recalled. IT performance was also an issue with slow electronic health record (EHR) system response times.

THE STRATEGY: Wiora noted a disconnect between the state of IT and Creative Solutions' passion for patient care. The company, based in Fort Worth, Texas, runs more than 49 skilled nursing and 13 assisted living facilities. The CIO determined cloud computing would let the IT side catch up. The company selected VMware's vCloud Air, an infrastructure as a service offering, as its core cloud technology. VMware, Wiora said, was open to accommodating Creative Solutions' security vision: a customized version of the Health Information Trust Alliance framework, which incorporates HIPAA, NIST, PCI and other security controls.

THE RESULTS: Incorporating the key frameworks into its cloud from the start put Creative Solutions on the proper security track. Plus, cloud improved the performance of applications such as EHR; instead of a two-second lag, round-trip latency is now in the 40 to 80 millisecond range. That's a big plus for care delivery—caregivers at a single facility use kiosk computers to record around 42,000 patient interactions daily. The company also addressed internet outages, using Cradlepoint technology that fails over to 4G in the event of disruption. "The company is now a phoenix out of the ashes in terms of IT," Wiora said. —JOHN MOORE

5 MINUTES WITH LINDA TUCCI

The Cyber Bad Guys Get Better

MIT Sloan cybersecurity expert Stuart Madnick talks about how dark web hackers continue to have the upper hand against enterprises.

BY LINDA TUCCI

STUART MADNICK

IN THE ONGOING and increasingly vicious cyberattacks against the world's best-known brands, the bad guys have it easier. So says Stuart Madnick, the John Norris Maguire Professor of Information Technologies at the MIT Sloan School and a speaker at the MIT Sloan CIO Symposium. Madnick, who currently serves as the director of the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, or (IC)3, explains how dark web hackers use technology and information to their advantage, as well as how marketplace pressures, the newness of the technology and human error make

HOME

IoT-enabled infrastructure vulnerable to attack.

How are businesses doing in the fight against cyberattacks? They have to be getting better.

It is true, people often observe that we are getting better. The thing that we often don't take note of is the bad guys are getting better even faster. That's the challenge. So I guess, indeed, things are getting better, but unfortunately, the worst is getting worster, if there's such a word. (Actually, I'm from Worcester, Mass., so I suppose that's appropriate.)

What is allowing the bad guys to get better and preventing the good guys from keeping up?

One of the things is that badness is getting commoditized, and that is the thing that used to be extremely exotic, requiring a Ph.D. in computer science to break into systems and so on. Now, it is available for sale on the dark web for $14.95. The tools and techniques that the hackers have available are increasingly available and becoming more powerful at an increasing rate.

Another thing I have observed in our research is the good guys actually do a bad job of sharing information. Now, when places like Target get attacked, they are required by law—because personal data is disclosed—to report it. And so it tends to get out into the press. But if, for example, a German steel mill is attacked and partially melts down, there's no obligation to report that publicly. In fact, even though Bloomberg reported it, they denied it ever happened.

The good guys keep it quiet for lots of reasons. They don't want the bad reputation. They don't want to encourage what I call copycat intruders. On the other hand, the bad guys have fantastic information-sharing arrangements on the dark web, so that's part of the reason why the bad guys are getting badder faster than good guys are getting gooder.

So, the dark web hackers have the upper hand. You'd think there would be a mechanism for easily sharing information without risking damage to a company's reputation or setting up copycat attacks.

I don't want to say there aren't attempts. In fact, if anything, there is a plethora of organizations trying to do the sharing. Unfortunately, they are extremely fragmented. What I'm about to say I'm not sure if I'm allowed to repeat publicly, but, apparently, the big oil companies actually do get together and share information, but only the bigger ones. They won't share it with the next level down, because they just want to keep it in a closed community.

It's the same reason why the FBI doesn't like sharing with the CIA, because they assume the CIA has moles in it and they'll leak everything out. The CIA doesn't want to share with the FBI because they're afraid the FBI has moles in it

and will let their stuff leak out.

Not that there aren't people trying to do it, but they're constantly getting tied up in these knots: 'If I reveal this, it will get exposed to the public. Will bad things happen to me?'

It's a bit ironic, if you think about it. The bad guys actually like reputation. 'I'm the one who broke into XYZ Bank and stole the billion dollars.' That's an ego thing to some extent. So, there are lots of reasons that those on what I'll call the dark web actually seek, if you will, publicity.

Can you give an example of an information-sharing network in the dark web ecosystem?

I don't know the name of it, but there actually is a website where the people of the dark web rank the most hated companies in the world. And you see a correlation: As your rating goes up to the top, the number of cyberattacks goes up, because a fair number of people don't attack for personal gain or for a nation-state. They just happen to like to show their anger about things. As your rank goes up, you find the number of these people in their spare time saying, for example, 'Monsanto is an evil company. I'm going to teach them a lesson. I'm going to bring them down.'

I was told that some companies actually hire other people to go in the dark web to vote them down lower as one way to reduce the number of attacks they see.

You moderated a session at the MIT Sloan CIO Symposium on mitigating cyber risks associated with internet-connected devices. Talk about the ways in which the internet of things (IoT) complicates the threat landscape.

Various estimates are that within a few years, there will be over 100 billion internet-connected devices, IoTs. It's one thing to go and try to lock 1,000 doors; imagine trying to lock 1 million doors or 100 billion doors. So, the number of attack surfaces is rapidly increasing.

There's another problem that will hurt us in several different ways. A year ago, I was on sabbatical and I spent part of my time at the University of Nice working with some people in the automotive telemetrics group. They were trying to do things that have never been done before, like autonomous driving and so on.

What I learned is that doing those things is extremely difficult. They are under tremendous constraints regarding the cost of the components, regarding the amount of energy they can consume, regarding the size of space they can take up. There's a whole long list of extremely challenging engineering problems they are wrestling with. If you have the top list of N priorities, cybersecurity, at least a year ago, was N+1. There were just so many things they had to deal with that they had to say, 'We'll focus on these now and worry about these others later.'

Part of the issue is the IoTs are so new, and there are so many challenges for the good guys in terms of trying to get them to work at all, that thinking really hard about cybersecurity is extremely difficult to factor into that.

So, the IoT security component is not built in from the beginning and more an afterthought at this point?

It is slowly changing. But as of a year ago, that was the case, and I think that's still probably the case of the majority of IoT work.

One of my colleagues works as a consultant. He worked for a company that was coming out with some IoT device. They were coming out with this device and they had just come to the realization that it was subject to certain types of cybersecurity attacks they hadn't considered before.

They realized that the computing power they had in their design would not allow them to make the software changes that would make the product more secure. They were faced with a decision. Do we release the product as planned this month or do a redesign, which could take six to eight months and possibly lose the market?

I'll let you speculate what decision they made. Hint: The product came out.

People like you are thinking hard about attacks on IoT-enabled infrastructure. Can you give me an example?

One example is the Turkish pipeline explosion, which, once again, Turkey denies was a cyberattack and claims it was just a malfunction. But according to other analysts, it was a cyberattack. But what's interesting about it was the cyberattack apparently originated through the security cameras that had recently been added to the pipeline.

So, the security camera, rather than being a security device, actually was the access device. Ironically, amongst the things the intruders did besides cause the pipeline to explode was, allegedly, they erased the security tapes as well and they cut down the alarm system. I was told that the only reason why the Turkish central control people knew a fire had broken out was when someone saw the fire blazing in the sky four miles away.

I mention this incident because one of the hot items being sold nowadays are these internet security cameras you can put outside your house or inside your house or as part of your baby monitoring and so on. I was told that 50% of all those devices still have the default pass code on them.

Is the U.S. government investing enough in protecting critical infrastructure?

Well, on the positive side, you may have seen that President Obama just announced ... an increase to $19 billion on cyber. So, at least there's more and more money being spent.

Our concern though is that a lot of the effort is—maybe

misdirected is too strong a term—is not adequately being directed because of a fantasy that if only I could come up with a better cryptographic code, all the problems will go away. And so they're not addressing hardly any of the organizational, managerial, cultural problems.

The organizational and cultural issues linked to cybersecurity is a big research focus at the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, or (IC)3, where you serve as director.

What we're focused on very much is the human element. Various reports have indicated that 50% to 70% of all cyberattacks are aided or abetted by insiders. Now, I can take that broadly. If you, as a homeowner, don't change that security code on your security camera when you buy it, I would argue you were a contributor to the cyber break-in. The actions or inactions of humans are by far the major issue. Putting a stronger lock on your door doesn't help if you're giving keys away or leaving a key under the mat.

So that's why, in our research, we're looking much more at the managerial and organizational aspects, which don't get much attention at all.

Like what?

Let me answer that by giving a couple of examples of things we're working on along that line. I'm at the Sloan School at MIT, and the adjacent building to us has been going through renovations for the last year or two. And for a long time, there was scaffolding on the outside. If you had been at MIT four or five months back, you would have seen on the scaffolding a big 10 foot-by-10-foot poster mounted. It had a picture of a worker, and in his hands, he's holding a photograph of his family. And above him is a sign that reads, 'I know why safety is important.' The implication being is, 'My family relies upon me. If I'm not safe, I'll be injured and that will harm my family.'

If you go into a factory, most likely you will see over the door a sign that says something like '570 days since last industrial accident.' When was the last time you went to a computer room and saw a sign over the door, '50 milliseconds since last successful cyberattack?'

That's a long introduction to saying what we're doing is trying to create what we call a cyber-safety discipline.

I read that your work on cyber safety is based on an MIT model called STAMP (Systems Theoretic Accident Modeling and Processes)—an approach to minimize and mitigate industrial accidents.

Yes, STAMP is obviously one of the main sources. STAMP is something MIT had been working on for approximately 20 years. It was used to analyze the Challenger space shuttle explosion.

How does STAMP apply to cybersafety?

There's several aspects of it. When you look at most mini cyber break-ins, or any kind of accident in general, you'll often hear the end result being human error. 'She left her password written on a note on her desk,' or whatever it might be. And the issue stops there.

We believe, in most cases, people don't deliberately want to create either industrial accidents or cyberevents. Usually, it is the incentive systems and organizational structure and culture that surrounds them that really has a lot to do with how people operate. That's the overarching thing of what STAMP started off doing and we're doing in cybersafety.

A Artificially Intelligent Attorney

An artificially-intelligent attorney is a legal expert system that applies AI to replicate and improve upon the abilities of a human legal research assistant. ROSS is an AI lawyer that began life as a research program at the University of Toronto. It is built on IBM Watson, mining data from about a billion text documents, analyzing it and providing precise responses to complicated questions.

D Deception Technology

Deception technology is a set of security tools and techniques designed to prevent an attacker who has already entered the network from doing damage. The technology uses decoys to misdirect the attacker and delay or prevent him from going deeper into the network. The products work by distributing deception decoys that mimic genuine IT assets and notify a special dedicated server called an engagement server or a deception server.

O Obfuscation

Obfuscation is the practice of making programming code hard to understand, often to protect intellectual property and prevent an attacker from reverse-engineering a proprietary software program. Obfuscation may involve encrypting some or all of the code, stripping out potentially revealing metadata or renaming useful class and variable names to meaningless labels.

R Rogue Employee

A rogue employee is a worker who undermines the organization that employs him by failing to comply with business rules and policies. The rogue worker might openly flout company rules or covertly subvert the company while attempting to escape detection by appearing compliant. In the worst-case scenario, a rogue employee is an insider threat, possibly engaging in industrial espionage and sharing sensitive corporate data with a competitor. ■

The Evolution of Cyberthreats

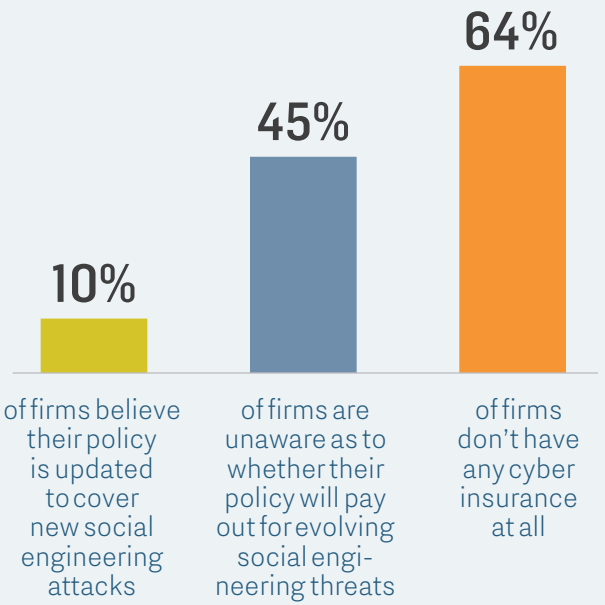
AS THE SOPHISTICATION and motivation of hackers continue to evolve, so do the range and frequency of criminal cyber activities, which range from hacktivism to social engineering to ransomware attacks. Here, we home in on the latter two of these cyber schemes, which are growing increasingly problematic for enterprises.

$30 MILLION

Amount in ransom the CryptoLocker cyber gang grossed in 2015

SOURCE: DELL SECUREWORKS THREAT ANALYSIS

CYBER INSURANCE: ARE YOU COVERED?



SOURCE: RESEARCH FROM MIMECAST LTD. (436 IT PROFESSIONALS SURVEYED)

FRAUD AND RANSOMWARE IN 2015

$1.07 BILLION

Losses from cybercrime ranging from hacktivist attacks to credit card fraud

$1.6 MILLION

Losses resulting specifically from ransomware infections

SOURCE: "2015 INTERNET CRIME REPORT," FBI INTERNET CRIME CENTER

67%

of companies that have seen a spike in "whaling" attacks, or CEO fraud

SOURCE: RESEARCH FROM MIMECAST LTD. (436 IT PROFESSIONALS SURVEYED)

Jason Sparapani
Features Writer

Falling Into the Skills Gap? Try Something New

AS ORGANIZATIONS SMALL and large turn to digital business models, many are looking at new ways of identifying and acquiring the right people to run them.

At the 2016 MIT Sloan CIO Symposium in Cambridge, Mass., three executives shared their organizations' views on talent acquisition in the digital age and the innovative methods they're using to close what's widely seen to be a tech skills gap—from using data to pinpoint job candidates to looking beyond four-year universities and colleges.

George Westerman, principal research scientist at the MIT Initiative on the Digital Economy, said typically when the economy is good, there are lots of job openings and low unemployment. Conversely, when the economy is slow, the number of job openings goes down and unemployment rises. But "something weird happened in 2009," he said. It was in the thick of the Great Recession: While unemployment remained high, the number of job openings swelled.

The skills gap is a common theme in IT: high demand for the right combination of technical, supervisory and communication skills and supply that can't keep pace.

A COLLEGE TRY

It's evident to Steve Phillips, CIO at Avnet Inc., which sells electronics components. He sees a shortage of "great technical people" who have an equal dose of business savvy.

He's also worried about getting the best crop of new graduates for the business. Avnet, in Phoenix, is more than 700 miles from Silicon Valley, but it still has to compete with the draw of the technology mecca's high salaries and cultural cool.

"Boy, it's like a magnet. It sucks up resources, Silicon Valley does," Phillips said.

So the company strengthened bonds with nearby Arizona State University, building deeper relationships with professors and students and opening the floodgates to its intern program. It has worked well so far, as the company now has more summertime interns than it is looking to hire.

"We're out there marketing ourselves to the university, to the students of the university. And I still think we've got a ways to go," Phillips said.

UNBLINDING WITH SCIENCE

Karen Kocher, chief learning officer for health insurance company Cigna, said it's not only a challenge to find candidates with technology and business skills. Finding IT people who can collaborate with others in the organization and understand the wants and needs of customers is especially tough. Those aren't traits that are visible to the naked eye.

> **"The supply-and-demand calculus of job-candidate skills is more 'market failure' than tech skills gap."**
>
> —GERALD CHERTAVIAN, *Boston nonprofit Year Up*

"If you were to ask us who are the influencers in our organization, most of the people that we would name—at least half of those would be incorrect," Kocher said. In other words, you might think you know the characteristics of the people who influence others, but you're probably wrong.

To find the skills it wants for its workforce, Cigna bases searches on hard data. It uses tools such as organizational network analysis, a quantitative technique for studying communication, "to really uncover people that are influencers, that are connectors and brokers and understand the importance of that, understand their aptitude in that and how to develop others to be more like that."

CIOs, she said, could play a pivotal role in drawing attention to and implementing such data-based recruiting methods.

DIAMONDS IN THE ROUGH

Gerald Chertavian, CEO and founder of Boston nonprofit Year Up, which matches low-income young people with training and jobs, said the supply-and-demand calculus of job-candidate skills is more "market failure" than tech skills gap.

When employers look at college-educated candidates, he said, they're typically thinking of students between the ages of 18 and 22 who earned a bachelor's degree in four years. But that's a small percentage, he said—just eight out of 100 Americans.

"So the question is: How are we looking at talent? How are we determining who's talented?" he said. "What proxies are we using for that which may or may not introduce a lot of bias?"

Year Up gives 18 to 24 year olds who were "not born in the right ZIP code" six months of professional and technical training and then helps them get internships and jobs with companies such as Citigroup, Facebook and Google. The program teaches technology topics such as JavaScript,

networking and hardware repair as well as business skills like writing and time management.

"Our most forward-thinking employers are looking more broadly at pathways into their organizations that are not myopically focused on what higher education and post-secondary education used to look like as opposed to where it's headed in the next 20 years," Chertavian said.

SECURING THE FUTURE

His message resonated with Vineeta Kumar, a consultant at global outfit Wipro. She cited cybersecurity as one of the most important areas of concern for any digital organization. The tech industry has "come up pretty fast" in cultivating security skills, but there still aren't enough people today who know how to deal with the volume of information that needs to be deciphered and analyzed.

The problem could be cracked, Kumar said, by looking not just at students graduating from four-year universities and colleges but from specialized courses and certification programs such as Khan Academy, a nonprofit that offers free education through YouTube videos.

That, she said, would help distribute jobs to more of the people who can do them.

"Not everybody has the ability, just the way the system works, to go and take out a college loan and go through four years and have to repay it," Kumar said. "These online universities and courses that are very specialized help you land a decent job in a large corporation. I think that's going to help." ■

Blockchain Under Scrutiny

"I think that cryptocurrencies is 1% of the uses of blockchain. ... It happened to be the first use case, but is 1%."

ARVIND KRISHNA, *Senior Vice President and Director of Research, IBM*

"What you don't want is what has happened in the OpenStack world, where it's just a bunch of convoluted challenges that are being gradually overcome but many chefs spoiling the soup. So you don't want blockchain to suffer from that type of confusion."

CARL LEHMANN, *Analyst, 451 Research*

"It is important to note that private blockchains are not a solution to privacy. ... If your primary information security concern is that you want privacy, and you are not interested in getting into advanced crypto or at least moderately complex crypto-economic mechanisms ... then you likely want a server and not a blockchain."

VITALIK BUTERIN, *Founder, Ethereum*

"The risk is that people will not be patient and will switch to something else; the recent rapid rise in developer interest and price of Ethereum should be a warning."

GAVIN ANDRESEN, *bitcoin core developer, on the threat bitcoin faces if its block size limit is not increased to 2 MB soon*

"I will make the argument right now that only six or seven of my brothers and sisters [in Congress] even understand the basic mechanics of the distributed ledger."

DAVID SCHWEIKERT, *U.S. Rep., R.-Arizona, at the DC Blockchain Summit*

Join the conversation
twitter.com/searchcio
facebook.com/searchcio

ABOUT THE AUTHORS

LINDA TUCCI

is executive editor of SearchCIO.
Write to her at ltucci@techtarget.com.

JOHN MOORE

is senior site editor for SearchITChannel.
Write to him at jmoore@techtarget.com.

SUE TROY

is editorial director of SearchCIO.
Write to her at stroy@techtarget.com.

COVER IMAGE: MARABELO/FOTOLIA

TechTarget

CIO Decisions is a SearchCIO.com e-publication.

Sue Troy
Editorial Director

Linda Tucci
Executive Editor

Francesca Sales
Site Editor

Nicole Laskowski
Senior News Writer

Jason Sparapani
Features Writer

John Moore
Contributor

Linda Koury
Director of Online Design

Marty Moore
Senior Production Editor

For sales inquiries:
Amalie Masucci
Director of Product Management
amasucci@techtarget.com

WEBSITE Visit us | EMAIL Contact us | TWITTER Follow us | FACEBOOK Connect with us | GOOGLE PLUS Add us

TechTarget USA
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.