



## 9 Strategic IT Planning Templates

Reach your business goals and stay organized by using one of these 9 FREE templates already in use by major organizations such as NASA, Brown University and the City of Ottawa

**ADOPT AND CRAFT YOUR IT PLAN WITH THE GUIDANCE OF YOUR PEERS**

[Download Now](#)



## Essential Guide

### An IT security strategy guide for CIOs

A comprehensive collection of articles, videos and more, hand-picked by our editors

# Congress questions blockchain security amid ransomware news



by  
**Francesca Sales**  
Site Editor

Published: 18 Mar 2016



Spreading cybercrime, like the ransomware attacks on NYT and BBC, has Congress considering Bitcoin security. Also in Searchlight: Apple might boost iCloud encryption; Amazon eyes selfie payments.

**ADOPT AND CRAFT YOUR IT PLAN WITH THE GUIDANCE OF YOUR PEERS**

## 9 Strategic IT Planning Templates

Reach your business goals and stay organized by using one of these 9 FREE templates already in use by major organizations such as NASA, Brown University and the City of Ottawa

[Download Now](#)

FROM THE ESSENTIAL GUIDE:

**An IT security strategy guide for CIOs** »

### GUIDE SECTIONS

1. IT security strategy overview
2. Security culture
3. Mobile security

[+ Show More](#)

This past weekend, security researchers discovered that some of the world's most popular and far-reaching websites,...

[Sign in for existing members](#)

## Continue Reading This Article

Enjoy this article as well as all of our content, including E-Guides, news, tips and more.

corporate email address

Continue Reading

By submitting your email address, you agree to receive emails regarding relevant topic offers from TechTarget and its [partners](#). You can withdraw your consent at any time. Contact [TechTarget](#) at 275 Grove Street, Newton, MA.

You also agree that your personal information may be transferred and processed in the United States, and that you have read and agree to the [Terms of Use](#) and the [Privacy Policy](#).



including AOL, BBC, MSN and The New York Times, exposed their customers to ransomware via their online ads. The incident, unfortunately, isn't unprecedented. The problem of ransomware, in fact, is on the rise -- and the U.S. government is appraising the digital currency that is associated with this cybercrime.

Malicious advertisements, which trick victims into installing ransomware and other types of malware, have also recently hit [Forbes](#) and [Yahoo](#). RiskIQ, a cybersecurity company in San Francisco, [reported](#) the number of unique malvertisements in June 2015 rose 60% from the same time the year before. Ransomware, in particular, is spiking rapidly: According to McAfee Labs' August 2015 [Threats Report](#), this type of cyberextortion grew 58% in the second quarter of 2015, compared with Q2 of 2014.

The criminals who unleash ransomware encrypt victims' data and [demand payment in bitcoins](#) in exchange for the decryption key. The burgeoning problem of ransomware, combined with the lack of regulation around the cryptocurrency [Bitcoin](#) and its underlying technology, has started to draw the attention of U.S. legislators.



**TOP CIO'S REVEAL THEIR BIGGEST IT ISSUES**

**7 IT executives, 7 Different Challenges**

CIO's from prominent organizations such as Verizon and Fidelity explain how they overcame some of their toughest challenges

**Download Now**

[Blockchain](#), the distributed ledger technology that underpins Bitcoin and other digital currency transactions, has been in use for eight years. However, the promise and [potentially disruptive effects of the technology](#), particularly in the finance and legal fields, has only recently reached Congress' awareness, with legislators such as [Rep. David Schweikert](#) (R.-Ariz.) calling for greater education among their peers.

## PRO+ Content



### E-Zine

[The key steps to launching blockchain implementations](#)



### E-Handbook

[Pondering the question of IoT data ownership](#)

**Find more PRO+  
content and other  
member only offers,  
here.**



### E-Handbook

[Hyper-converged infrastructures:  
Game changer or vendor push?](#)

But given the lack of awareness in Congress around blockchain, and the role of Bitcoin in cybercrime and terrorism, other legislators are currently focused more on blockchain security and the risks associated with the technology, as opposed to its potentially good uses. In a [testimony on the topic](#) that was held before the House Subcommittee on Commerce, Manufacturing and Trade on Tuesday, committee members expressed their concern that blockchain enables cybercriminals by giving them a way to transfer money that is hard to trace by law enforcement.

"It isn't like a bag of bitcoins can be taken down to the wharf and left under a boat," said Michael Burgess, the subcommittee's chairman. "When I questioned, 'Well, why don't you just follow the [digital trail](#)?' Well, you can't do that. ... Could you enlighten the subcommittee on the law enforcement aspect?" he asked the witnesses, who comprised blockchain experts from various fields.

Witness Jerry Brito, executive director of Coin Center, a public policy organization dedicated to digital currency research, acknowledged that ransomware is a very serious problem made possible by Bitcoin, as well as

cryptography and data breaches.

But he and fellow witnesses stressed that despite the negative uses of cryptography, cryptocurrencies and blockchain, they **also come with important benefits**. Cryptography, for example, helps keep sensitive financial data safe. And blockchain architecture could be applied more broadly to assets other than virtual currency, such as land deeds, birth certificates and sale contracts.

"It is attractive to start thinking about the blockchain as something that is permissioned, not just anonymous," said Gennaro Cuomo, vice president of blockchain technology at IBM, whose Global Financing division runs its transactions on blockchain. "For example, two parties exchanging car VIN numbers may have a certain level of permissions. Maybe one is an auto manufacturer, maybe the other is an auto dealer. You might be able to see those cars that only pertain to your transaction. ... But the Department of Motor Vehicles, when it comes to the door of the car club, is given broader permissions as an auditor in that blockchain network."

The problem doesn't lie with Bitcoin or blockchain, they said. Instead, it's more about cybersecurity.

"The third component of ransomware -- the breach, the hack, the lack of cybersecurity -- that's where the real concern is," Brito said.

Dana Syracuse, counsel at BuckleySandler LLP, based in Washington, D.C., agreed, saying Bitcoin itself -- as well as other virtual currencies -- is highly traceable using blockchain forensics that can follow the flow of transactions.

"This allows one to follow transactions using blockchain forensics from one exchange to another or from wallet to wallet."

**This traceability** is what keeps the use of Bitcoin for terrorist financing and money laundering, one of the major concerns brought up by the subcommittee, to a minimum.

"Those are the very fringe use cases," said Matthew Roszak, chairman of the Chamber of Digital Commerce, a trade association. "Digital currency,

especially Bitcoin, is not a great use of funding for criminal activities."

Brito concurred. "To date, we have not seen terrorist financing using digital currency. ... Cash is still the No. 1 way people conduct terrorist financing," he said.

What Congress and law enforcement need to be looking at instead is the "on-ramp" and the "off-ramp" of the people making these transactions -- their entry and exit points, respectively -- and make sure these are regulated, according to Syracuse.

"It is a story about cybersecurity. It's a larger conversation that needs to be had around regulation in that area and creating proper standards there," Syracuse said. Furthermore, it's important that law enforcement officials [educate themselves](#) on the forensics tools available, so they can trace funds, he added.

**It is a story about cybersecurity. It's a larger conversation that needs to be had around regulation in that area and creating proper standards there.**

Brito also advised steering [the blockchain security conversation](#) to the *uses* of

**Dana Syracuse**  
counsel, BuckleySandler

cryptocurrencies, emphasizing the value of educating law enforcement on tools that are available to track these transactions. He pointed to the role of public and private forums, such as the Blockchain Alliance: The forum, which was jointly formed by Coin Center, the Chamber of Digital Commerce and other companies, enables law enforcement and companies participating in digital currencies to discuss these topics.

So, what aspects of Bitcoin and its ecosystem should be regulated, and should they be regulated by existing money transfer laws?

The answer to this question is complex, as Syracuse laid out. In New York

point to another, but not the exchange companies or wallet companies.

Search the TechTarget Network

Other states' laws, however, could very well cover these other aspects, he said.

## Sections

CIO news roundup for week of March 14

When it comes to developing new regulations, Congress would need to

Next Steps

consider multiple factors in addition to cybersecurity, including

antilaunders and consumer protection, Syracuse added.

## Essential Guide

## Cyber



Francesca Sales asks:

More at section

Evaluate cybers

Wisconsin for cyber power

Burgeoning intensifying sharing

Sponsored

As Security Increased: Defense Are ...  
-Dell

2 Responses

Join the Discussion

Credit  
Cryptolocker Attack With Smart Backup Policy  
-SimpliVity

## CIO news roundup for week of March 14

Vendors

Blockchain security was only one of many eye-catching tech headlines this week:  
-LogRhythm

Computer 2016: A disaster  
-Comp

- In the latest round in Apple's privacy battle with the feds, the company said it wants to ramp up the [encryption of its iCloud](#) storage service without inconveniencing customers. There are some hurdles to overcome, however: Taking steps such as giving only the user the key to their encrypted data could mean trouble if the user loses that key, but if Apple keeps a second key, that copy could be compromised.

- Instagram is joining the likes of Facebook and Twitter and is [jumping on the algorithm bandwagon](#). The photo-sharing company is personalizing its feed based on an algorithm that will place photos it deems you will be most interested in at the top of your feed, instead of in chronological order. Many users [aren't keen](#) on the development, however.
- Amazon is so done with "awkward" passwords. The online retail giant has a filed a patent for [facial recognition technology](#) that would allow customers to authenticate payments by taking a picture or video of themselves instead of entering a password. On top of security, the company wants to improve UI: "The entry of these passwords on portable devices is not user-friendly in many cases, as the small touchscreen or keyboard elements can be difficult to accurately select using a relatively large human finger," said the company in a filing.
- Should you 3D-print your own cheap pair of braces instead of paying thousands at the orthodontist? Sounds too good to be true, but [one college student did it](#). Amos Dudley, a New Jersey Institute of Technology student, used the school's 3D printer to create the corrective retainers; 16 weeks was all it took to fix his snaggle tooth. Don't try this at home, though, orthodontists warned.

## ➤ Next Steps

Blockchain ledger is [essential to the programmable economy](#)

[Blockchain security mechanisms](#) fuel tech development

[Blockchain is a threat and a promise](#) to financial services industry



### Essential Guide

### An IT security strategy guide for CIOs

#### GUIDE SECTIONS

1. IT security strategy overview



2. Security culture

3. Mobile security

4. Cloud security

5. IoT security

6. Security budgets

**7. Security and the government**

8. Security and analytics

9. Glossary

## Related Discussions

Francesca Sales asks:

What do you think are the most promising aspects of blockchain and blockchain security? What do you think are the technology's biggest risks?

2 Responses So Far

Join the Discussion

 0 comments

Oldest ▼

Share your comment

☒ Send me notifications when other members comment.

Register or [Login](#)

E-Mail

email@techtarget.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. [Privacy](#)

-ADS BY GOOGLE

## El Capitan running slow?

[macpaw.com/CleanMyMac3](http://macpaw.com/CleanMyMac3)

That's easy to fix. Follow these 5 steps and speed up your Mac now!



### Latest TechTarget resources

COMPLIANCE

HEALTH IT

CLOUD COMPUTING

MOBILE COMPUTING

DATA CENTER

### Search **Compliance**



#### Industry gurus tackle blockchain privacy and digital identity

The decentralized nature of public blockchain has raised concerns about digital identity and blockchain privacy. A panel of ...



#### Experts wade through hype to shed light on blockchain security

Along with the hype, there have been plenty of questions around blockchain technology, particularly regarding blockchain security...

[About Us](#)

[Contact Us](#)

[Privacy Policy](#)

[Corporate Site](#)

[Experts](#)

[Reprints](#)

[Events](#)

[Guides](#)

[Opinions](#)

All Rights Reserved, [Copyright](#)  
2007 - 2016, TechTarget

[Advertisers](#)

[Archive](#)

[Photo Stories](#)

[Business Partners](#)

[Site Map](#)

[Videos](#)

[Media Kit](#)

[E-Products](#)