



BOB AINSBURY

*Chief Product Officer,
Granicus*



Closing the Cyber Security Gap

2017 Digital Communications Summit
(DCCComm17)

Bob Ainsbury



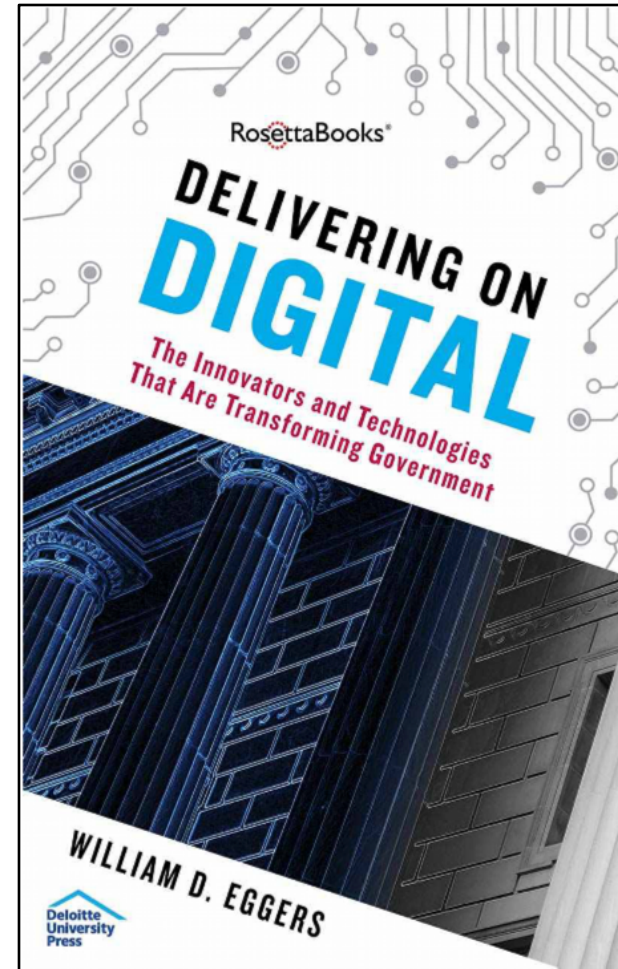
“The user's going to pick dancing pigs over security every time.”

The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals.

We cause accidents.


Those of us in security are very much like cardiologists. Our patients know that lack of exercise, too much dietary fat, and smoking are all bad for them. But they will continue to smoke, eat fried foods, and practice being couch potatoes until they have their infarction.

- **Social.** Allowing people to communicate electronically in real time
- **Mobility.** Connecting with people wherever they are
- **Analytics.** Using data to do sophisticated analysis across programs and policy areas
- **Cloud computing.** Storing and processing information on a network of remote servers, which changes how you use technology and how you pay for it
- **Cybersecurity.** Providing secure communication and data storage



- **Social.** Allowing people to communicate electronically in real time
- **Mobility.** Connecting with people wherever they are
- **Analytics.** Using data to do sophisticated analysis across programs and policy areas
- **Cloud computing.** Storing and processing information on a network of remote servers, which changes how you use technology and how you pay for it
- **Cybersecurity.** Providing secure communication and data storage





the practice of using a network of remote servers (accessed via the Internet) to store, manage, and process data, rather than a local system.



**YOUR STUFF ON OTHER PEOPLES SYSTEMS
POTENTIALTY ACCESSABLE BY MORE THAN
25 BILLION DEVICES**







10,000,000 IAPD



10,000,000 IAPD



20,000,000 IAPD

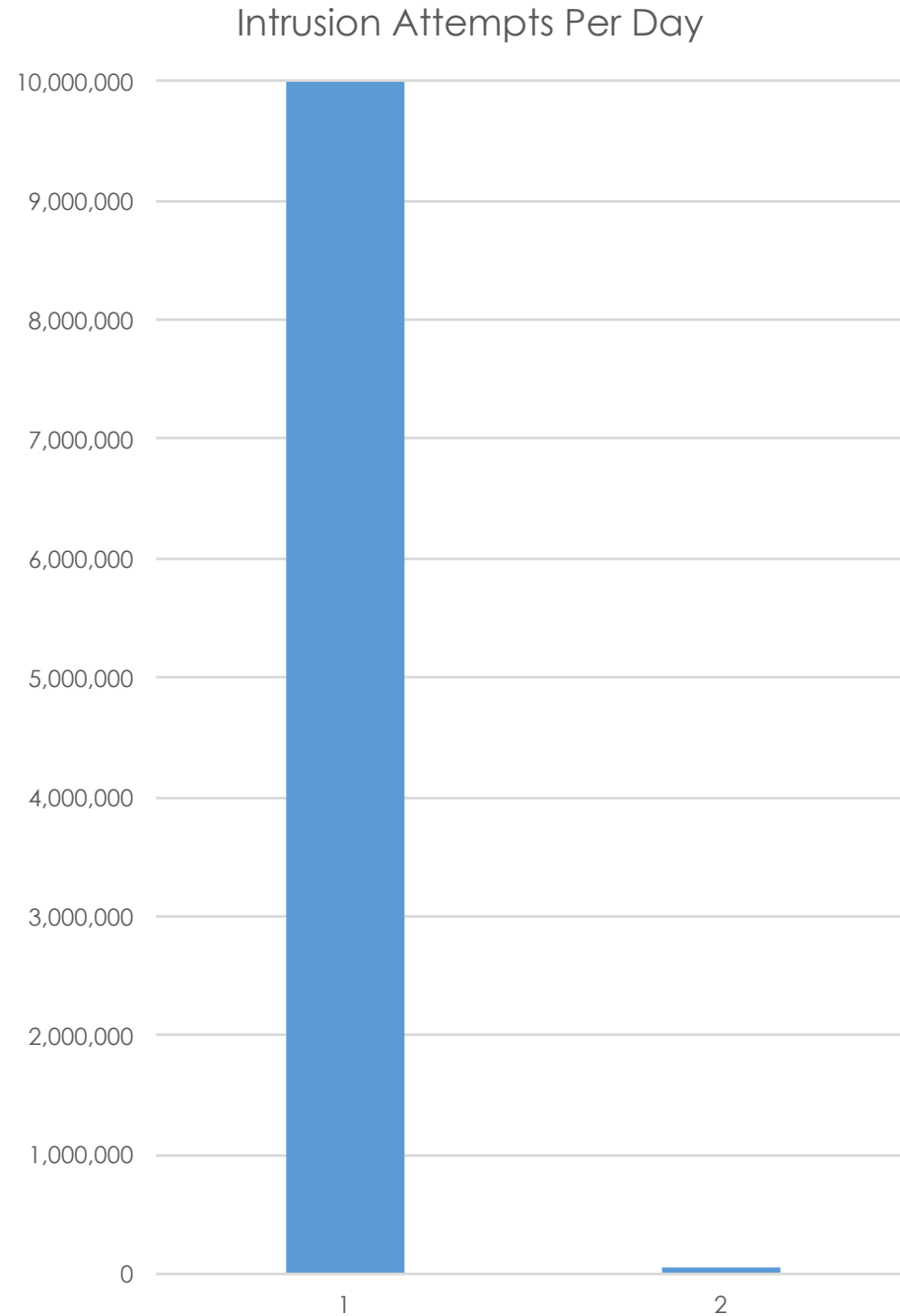
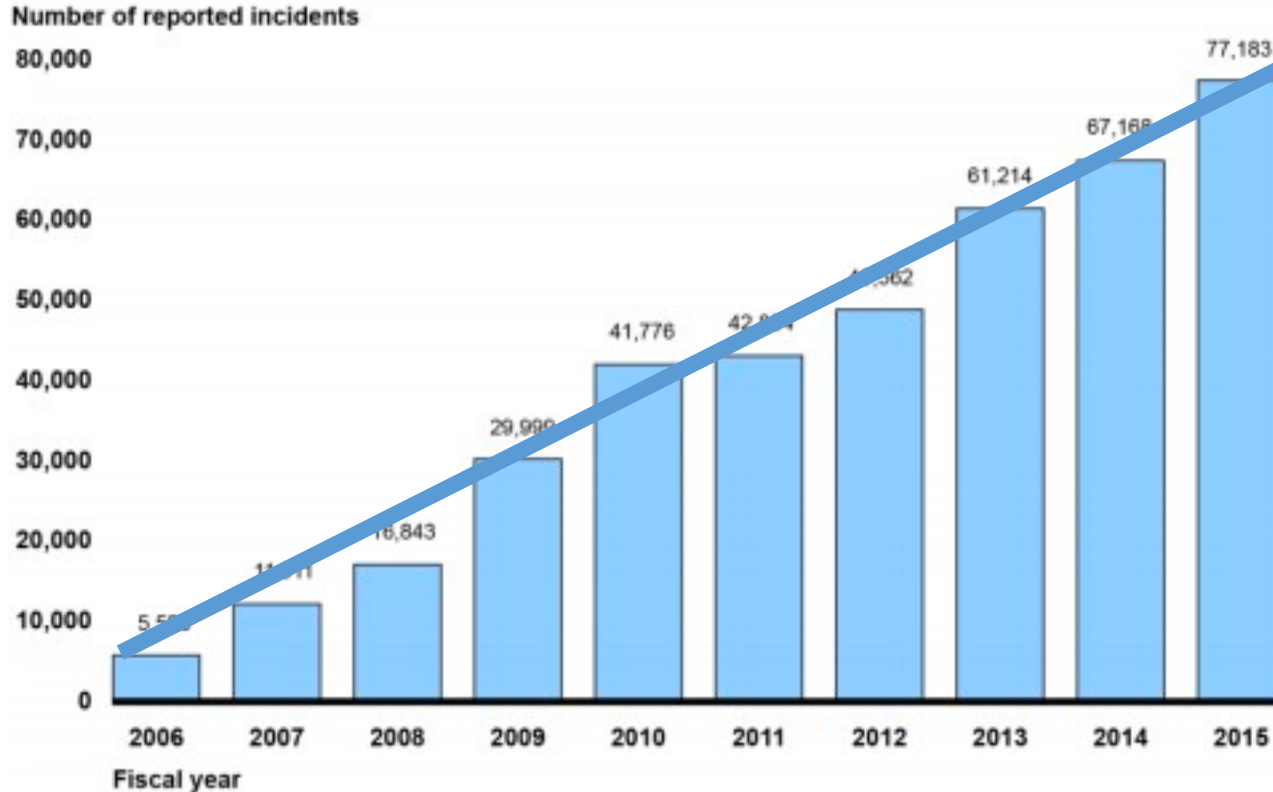


Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-501

1,300%

in February 2015, the Director of National Intelligence testified that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.

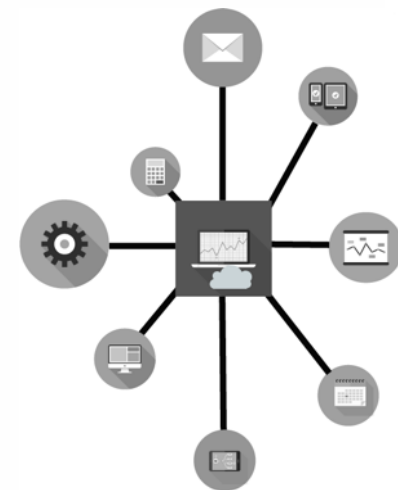
Chief Information Security Officer (CISO)

ensure that the agency is meeting the requirements of the law, including developing, documenting, and implementing the agency-wide information security program

Factor	Large extent	Moderate extent	Small extent	Not at all	No response
Competing priorities between operations and security	6	12	4	2	0
Coordination with component organizations	5	8	4	5	2
Coordination with other offices	3	9	3	9	0
Availability of information from contractors	4	8	10	2	0
Oversight of indirect reports	6	6	6	6	0
Oversight of IT contractors	4	8	6	6	0
Placement in organizational hierarchy	5	5	5	9	0
Availability of information from component organizations	5	4	10	5	0

Source: GAO analysis of survey data. | GAO-16-686

*We only need to be lucky once.
You need to be lucky every time.*



Do you exercise?

Do you smoke?

Do you drink?

How many hours do you sleep?

How stressful is your job?

When did you last go to the dentist?

When did you last take a vacation?



Do you exercise?

Do you smoke?

Do you drink?

How many hours do you sleep?

How stressful is your job?

When did you last go to the dentist?

When did you last take a vacation?



Do you receive regular security training?

Do you receive security incident alerts?

Do you share login credentials?

Is security discussed at team and group meetings?

Are there passwords on whiteboards?

Does your organization test employees for security IQ?




Do you receive regular security training?

Menu

- ▶ Security Awareness
- ▼ Network Access
 - Introduction
 - Who are you?
 - I belong
 - Security Checklist - Buildin...
 - Another newbie
 - Visitor registration
- ▶ Types of Information
- ▼ Keep It Clear and Clean
 - Potential problems**
 - Up close and keep secure
 - Confidential messaging
 - Security Checklist - Work A...
- ▼ Passwords
 - Password Requirements
 - Computer Login
 - Sharing workloads
 - Here's my password
 - Security Checklist - Passwo...
- ▼ PC and Laptop Security
 - Introduction
 - Code, Cookies & Ethical Use
 - Email Intro
 - Email Inbox
 - credit card
 - Forwarded email
 - CEO
 - LinkedTo
 - Security Checklist - Use of ...
- ▼ Going Mobile
 - Mobile Introduction
 - Malfunction
 - Free WiFi

Security Awareness - Updated 8/18/2016

Resources



It's easy to think of our work areas as secure. We're behind locked doors, and visitors are not allowed to move about freely. However, our information is only as secure as we choose to make it.

Click the locations where it's easy to allow information to be vulnerable.

(Hint: There are seven vulnerable locations.)

Help

◀ PREV NEXT ▶


Does your organization test employees for security IQ?

Message

FW: *****Office365 Account Updates Required***** - Temporary Items

Delete Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

FW: *****Office365 Account Updates Required*****

 Chris White <Chris.White@govdelivery.com>
Tuesday, August 23, 2016 at 10:40 AM
To: Jim Sarne

Hi Chris -

Due to the way Mimecast and Microsoft work together, a recent security update looks like it messed things up for some people. Sadly, you may be one of the unlucky folks. I need you to confirm whether the update has completed by **logging in to the secure Office 360 Mail**. It should only take a minute and will [really help me out](#). [Click here to help me make your email more secure!](#)

After you click the link and login, if you see the following image that means your account has been flagged as an incomplete upgrade and it will fix itself in 2-3 minutes.

If you login and see your email, then your account was already good. In either case, you don't have to do anything else after logging in!

We could do this ourselves, but since we're short staffed, this will help us out a lot. No need to contact us, we'll get the report directly from Microsoft.

And no, Chris White, this isn't a phishing email! If you want to waste my time by emailing me to confirm this, go ahead I guess, but it's a waste of time...

Once this is complete, we'll have more exciting Office365 news to share with everyone!

Thank you.

Susan

Does your organization test employees for security IQ?

Message

SECURITY: GovDelivery Phishing Results - Temporary Items

Delete Reply Reply All Forward Attachment Meeting Move Junk Rules Read/Unread Categorize Follow Up

SECURITY: GovDelivery Phishing Results

GovDelivery Internal Communications <gdinternal@public.govdelivery.com>
Tuesday, April 26, 2016 at 7:30 AM
To: Chris White

Statistics

So having said that, how did GovDelivery do as a whole on our first test? Overall, it was a mixed bag. The message was sent out at 6:05am and we had the following results:

- Messages: 217
- Opened: 153 (70.5%)
- Clicked: 21 (9.7%)
- First open: 6:15am
- First click: 6:20am
- Last click: 1:54pm
- First helpdesk report: 6:54am

Identification

If you were one of those 21 people who clicked the link, what clues were available to help you figure out that this wasn't actually an email from IT, but rather someone trying to do bad things to your computer? Let's look at the email. I've put red boxes around the pieces that look suspicious, and green boxes around the parts that make the message sound more legit.

Tue 4/19/2016 6:05 AM

IT

ACTION REQUIRED: Apple QuickTime and Java immediate upgrade!

To: Chris White

Salesforce

All GovDelivery employees:

Please notice that the federal government has recently issued a Security Update for Java and for Apple QuickTime and FEDRAMP requires we install them. The update applies to the following OS versions: Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 10, and all version of Apple OS X after Snow Leopard. Linux is probably not impacted, but check the KB article to make sure.

Please notice, that present update applies to high-priority updates category. In order to help protect your computer against security threats and performance problems, we require you to install this update. Because our automated tools did not fix the problem, we made a decision to issue an experimental private version update for all affected users.

As your computer is set to receive notifications when new updates are available, you have received this notice.

In order to start the update, please follow the step-by-step instruction:

1. Run the file, that you have received along with this message. KB958644-ENU

2. Carefully follow all the instructions you see on the screen.

http://https.file-transfer.ancillarycheese.com/cmyxaxbpzw50z2lkpt3odyjnty1myzjyw1wywlnbif9dw5fawqfmczmda4gmfdglvb1j8gjayz1cmw9ah0chm0by9ecm90zwm0cwgqzmy9wmyy29k3bh2vc2vmota3mtbh2gqvw

Click to follow link

Take a moment and think about yourself, your group, your department, your agency.

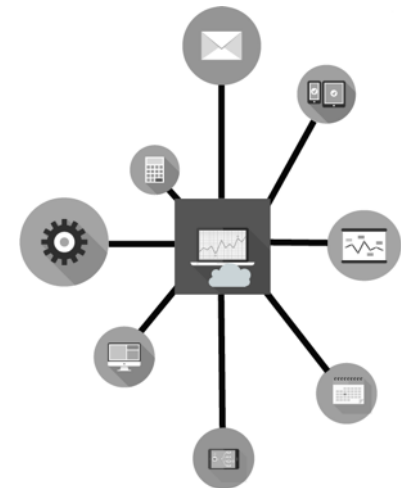
How do you rate your security health?

the systems you use need to be secure



FEDRAMP

provides a standardized approach to security assessment, authorization, and continuous monitoring





1. A company doesn't get authorized – individual products or services do.
2. Just because a product runs in a FedRAMP cloud provider (like Amazon) doesn't mean that the application is FedRAMP'dfar from it.
3. Agency's have to use FedRAMP'd solutions
4. FedRAMP uses a very rigorous and effective process
5. An agency has security obligations even when you use a FedRAMP'd Product

- Bulletins
- Campaigns
- Reports**
- Topics
- Segments
- Subscribers
- Subscriber Capture
- Categories
- Templates
- Macros
- Administrators
- Announcements
- Trash Can
- Themes
- Roles
- Featured Content
- Social Media
- Connect
- System

03/2017 ⓘ

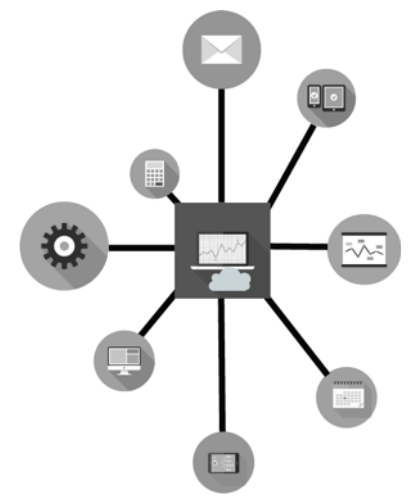
Security Compliance Officer

Summary

23 Admins Attempted to Login	95 Total Login Attempts	7 Failed Login Attempts	92.63% Login Success Rate	0 Lockouts
--	-----------------------------------	-----------------------------------	-------------------------------------	----------------------

Administrator Activity Top 15 entries (of 23 total) [CSV \(ALL\)](#)

EMAIL	ROLE	LOCKOUTS	FAILED LOGINS	LOGIN SUCCESS
[REDACTED]	Topic Administrator (Limited)	0	3	40.00%
[REDACTED]	Topic Administrator (Limited)	0	0	100.00%
[REDACTED]	Account Administrator	0	0	100.00%
[REDACTED]	Account Administrator	0	0	100.00%
[REDACTED]	Topic Administrator	0	0	100.00%
[REDACTED]	Topic Administrator (Limited)	0	0	100.00%
[REDACTED]	Account Administrator	0	1	75.00%
[REDACTED]	Topic Administrator	0	0	100.00%
[REDACTED]	Topic Administrator	0	0	100.00%



Closing the GAP

- Get security burned into your culture – don't wait for the CISO
 - Make security part of your regular dialog
 - Train and re-train
 - Test your teams
 - Measure, Monitor, Adjust
- Only use FedRAMP approved products
 - And do your part in meeting your obligations

Those of us in security are very much like cardiologists. Our patients know that lack of exercise, too much dietary fat, and smoking are all bad for them. But they will continue to smoke, eat fried foods, and practice being couch potatoes until they have their infarction.

Thank You!

Bob Ainsbury

Chief Product Officer

bob.ainsbury@granicus.com