Risky Business

IT Risks and How Analytics Can Help Mitigate Them

weaver

Assurance • Tax • Advisory

weaver
Assurance • Tax • Advisory

Your Presenters

Elisa Gilbertson, CPA

- Manager of Weaver Analytics
- Over 8 years of experience providing public accounting services; over 2 years experience in school district financial administration
- Practice emphasis in data analytics, auditing and consulting for a variety of industries including state and local government, nonprofit organizations and higher education.

Raveen Bhasin, CISM, CISA, ITIL, CSM

weaver
Assurance • Tax • Advisory

- Manager with Weaver’s IT Advisory Services practice
- A decade of experience in IT risk advisory services and attestation engagements including two years each with Deloitte & Touche and KPMG
- Extensive experience in software selection, platform design and implementation reviews, including SDLC process assessments focused on Agile, Scrum, Kanban and traditional Waterfall methodologies

Top IT Risks

- Administrative Access
- Segregation of Duties
- Terminated Employee Access
- Change Management
- Passwords
- Phishing

Administrative Access

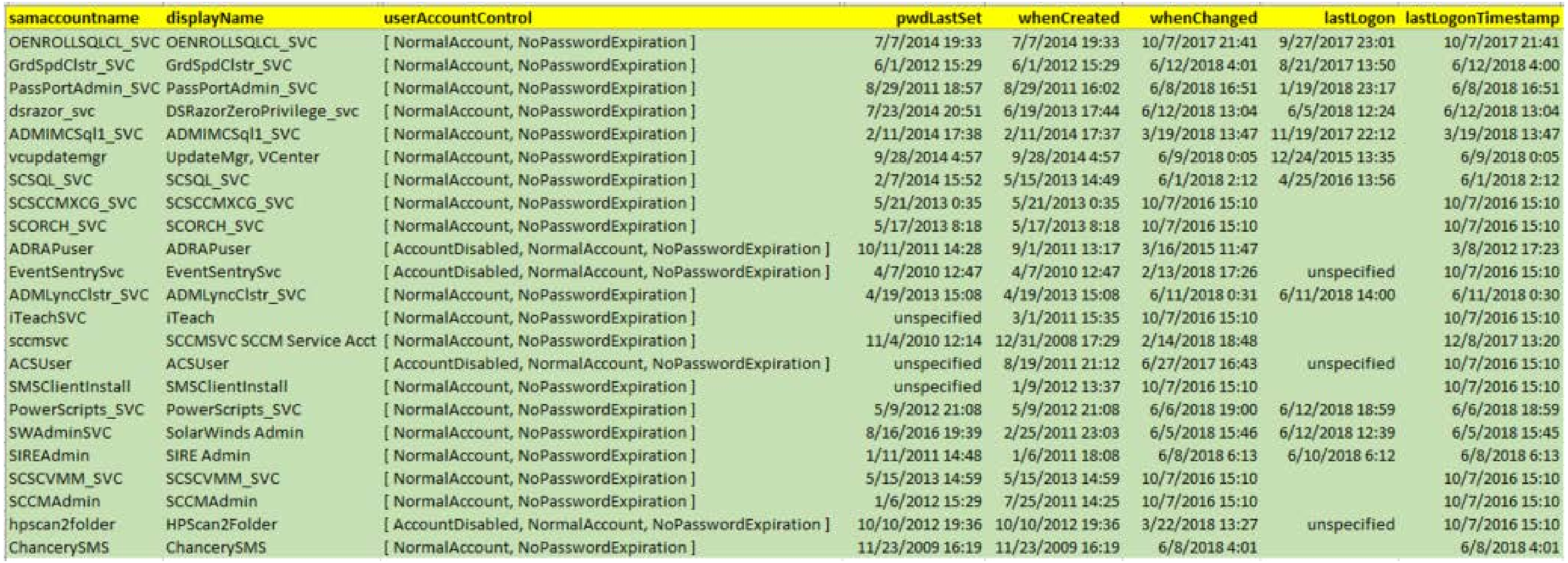
Administrative Access

- Administrators have keys to the kingdom
- Unmonitored access to perform changes – data and configurations
- Business users with admin access create a segregation of duties conflict

Administrative Access

- Administrator access at all layers matter – application, database, and operating system
- Ensure that access is truly limited to those who need it
- Create secondary accounts if non-IT back up personnel may require access and review usage (last login dates is an option)

Administrative Access



samaccountname	displayName	userAccountControl	pwdLastSet	whenCreated	whenChanged	lastLogon	lastLogonTimestamp
OENROLLSQLCL_SVC	OENROLLSQLCL_SVC	[NormalAccount, NoPasswordExpiration]	7/7/2014 19:33	7/7/2014 19:33	10/7/2017 21:41	9/27/2017 23:01	10/7/2017 21:41
GrdSpdClstr_SVC	GrdSpdClstr_SVC	[NormalAccount, NoPasswordExpiration]	6/1/2012 15:29	6/1/2012 15:29	6/12/2018 4:01	8/21/2017 13:50	6/12/2018 4:00
PassPortAdmin_SVC	PassPortAdmin_SVC	[NormalAccount, NoPasswordExpiration]	8/29/2011 18:57	8/29/2011 16:02	6/8/2018 16:51	1/19/2018 23:17	6/8/2018 16:51
dsrazor_svc	DSRazorZeroPrivilege_svc	[NormalAccount, NoPasswordExpiration]	7/23/2014 20:51	6/19/2013 17:44	6/12/2018 13:04	6/5/2018 12:24	6/12/2018 13:04
ADMIMCSql1_SVC	ADMIMCSql1_SVC	[NormalAccount, NoPasswordExpiration]	2/11/2014 17:38	2/11/2014 17:37	3/19/2018 13:47	11/19/2017 22:12	3/19/2018 13:47
vcupdatemgr	UpdateMgr, VCenter	[NormalAccount, NoPasswordExpiration]	9/28/2014 4:57	9/28/2014 4:57	6/9/2018 0:05	12/24/2015 13:35	6/9/2018 0:05
SCSQL_SVC	SCSQL_SVC	[NormalAccount, NoPasswordExpiration]	2/7/2014 15:52	5/15/2013 14:49	6/1/2018 2:12	4/25/2016 13:56	6/1/2018 2:12
SCSCCMXCG_SVC	SCSCCMXCG_SVC	[NormalAccount, NoPasswordExpiration]	5/21/2013 0:35	5/21/2013 0:35	10/7/2016 15:10		10/7/2016 15:10
SCORCH_SVC	SCORCH_SVC	[NormalAccount, NoPasswordExpiration]	5/17/2013 8:18	5/17/2013 8:18	10/7/2016 15:10		10/7/2016 15:10
ADRAPuser	ADRAPuser	[AccountDisabled, NormalAccount, NoPasswordExpiration]	10/11/2011 14:28	9/1/2011 13:17	3/16/2015 11:47		3/8/2012 17:23
EventSentrySvc	EventSentrySvc	[AccountDisabled, NormalAccount, NoPasswordExpiration]	4/7/2010 12:47	4/7/2010 12:47	2/13/2018 17:26	unspecified	10/7/2016 15:10
ADMLyncClstr_SVC	ADMLyncClstr_SVC	[NormalAccount, NoPasswordExpiration]	4/19/2013 15:08	4/19/2013 15:08	6/11/2018 0:31	6/11/2018 14:00	6/11/2018 0:30
iTeachSVC	iTeach	[NormalAccount, NoPasswordExpiration]	unspecified	3/1/2011 15:35	10/7/2016 15:10		10/7/2016 15:10
sccmsvc	SCCMSVC SCCM Service Acct	[NormalAccount, NoPasswordExpiration]	11/4/2010 12:14	12/31/2008 17:29	2/14/2018 18:48		12/8/2017 13:20
ACSUser	ACSUser	[AccountDisabled, NormalAccount, NoPasswordExpiration]	unspecified	8/19/2011 21:12	6/27/2017 16:43	unspecified	10/7/2016 15:10
SMSClientInstall	SMSClientInstall	[NormalAccount, NoPasswordExpiration]	unspecified	1/9/2012 13:37	10/7/2016 15:10		10/7/2016 15:10
PowerScripts_SVC	PowerScripts_SVC	[NormalAccount, NoPasswordExpiration]	5/9/2012 21:08	5/9/2012 21:08	6/6/2018 19:00	6/12/2018 18:59	6/6/2018 18:59
SWAdminSVC	SolarWinds Admin	[NormalAccount, NoPasswordExpiration]	8/16/2016 19:39	2/25/2011 23:03	6/5/2018 15:46	6/12/2018 12:39	6/5/2018 15:45
SIREAdmin	SIRE Admin	[NormalAccount, NoPasswordExpiration]	1/11/2011 14:48	1/6/2011 18:08	6/8/2018 6:13	6/10/2018 6:12	6/8/2018 6:13
SCSCVMM_SVC	SCSCVMM_SVC	[NormalAccount, NoPasswordExpiration]	5/15/2013 14:59	5/15/2013 14:59	10/7/2016 15:10		10/7/2016 15:10
SCCMAdmin	SCCMAdmin	[NormalAccount, NoPasswordExpiration]	1/6/2012 15:29	7/25/2011 14:25	10/7/2016 15:10		10/7/2016 15:10
hpscan2folder	HPScan2Folder	[AccountDisabled, NormalAccount, NoPasswordExpiration]	10/10/2012 19:36	10/10/2012 19:36	3/22/2018 13:27	unspecified	10/7/2016 15:10
ChancerySMS	ChancerySMS	[NormalAccount, NoPasswordExpiration]	11/23/2009 16:19	11/23/2009 16:19	6/8/2018 4:01		6/8/2018 4:01

weaver
Assurance • Tax • Advisory

Segregation of Duties

Segregation of Duties

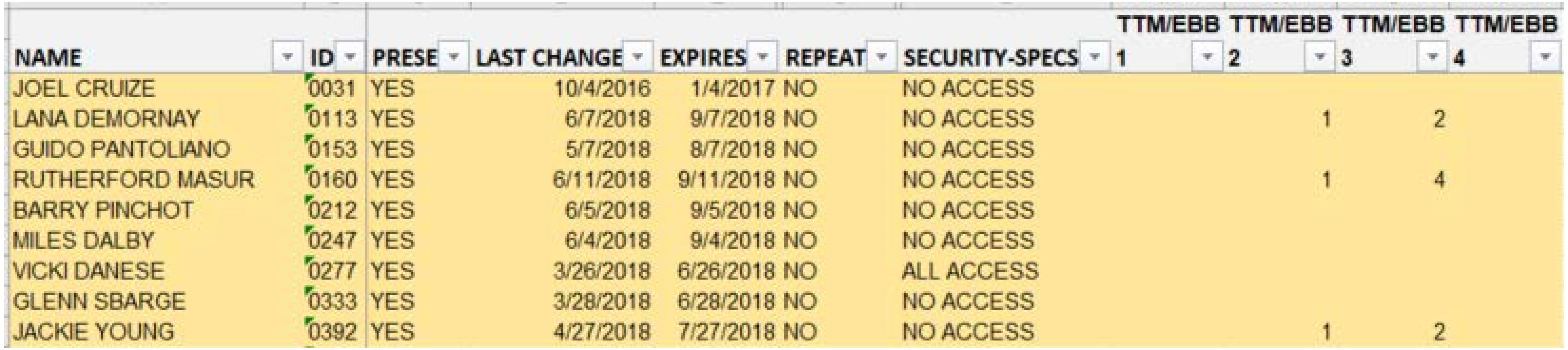
- Functional responsibilities, including backup responsibilities, may result in access segregation of duties conflicts
- Security roles in applications may not be set up with least privilege
- Access based segregation of duties is not defined and monitored
- Threatens reliability of authorization and oversight

Segregation of Duties

- Review role assignments to users
- Review permissions assigned to roles
- Position transfers – retaining both job duties' responsibilities
- Identify ownership of generic/shared IDs
- Create a segregation of duty monitoring process

Segregation of Duties

weaver
Assurance • Tax • Advisory



NAME	ID	PRESE	LAST CHANGE	EXPIRES	REPEAT	SECURITY-SPECS	TTM/EBB 1	TTM/EBB 2	TTM/EBB 3	TTM/EBB 4
JOEL CRUIZE	0031	YES	10/4/2016	1/4/2017	NO	NO ACCESS				
LANA DEMORNAY	0113	YES	6/7/2018	9/7/2018	NO	NO ACCESS		1	2	
GUIDO PANTOLIANO	0153	YES	5/7/2018	8/7/2018	NO	NO ACCESS				
RUTHERFORD MASUR	0160	YES	6/11/2018	9/11/2018	NO	NO ACCESS		1	4	
BARRY PINCHOT	0212	YES	6/5/2018	9/5/2018	NO	NO ACCESS				
MILES DALBY	0247	YES	6/4/2018	9/4/2018	NO	NO ACCESS				
VICKI DANESE	0277	YES	3/26/2018	6/26/2018	NO	ALL ACCESS				
GLENN SBARGE	0333	YES	3/28/2018	6/28/2018	NO	NO ACCESS				
JACKIE YOUNG	0392	YES	4/27/2018	7/27/2018	NO	NO ACCESS		1	2	

weaver
Assurance • Tax • Advisory

Terminated User Access

Terminated Users

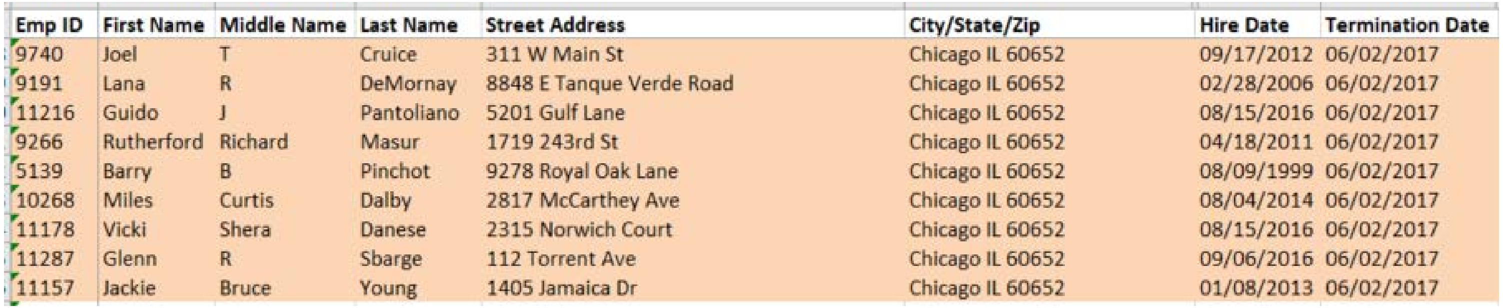
- Terminated employee's access is not revoked
- Active Directory / Novell layer
- Application layer
- Usage by terminated employee
- Usage by existing employees

Terminated Users

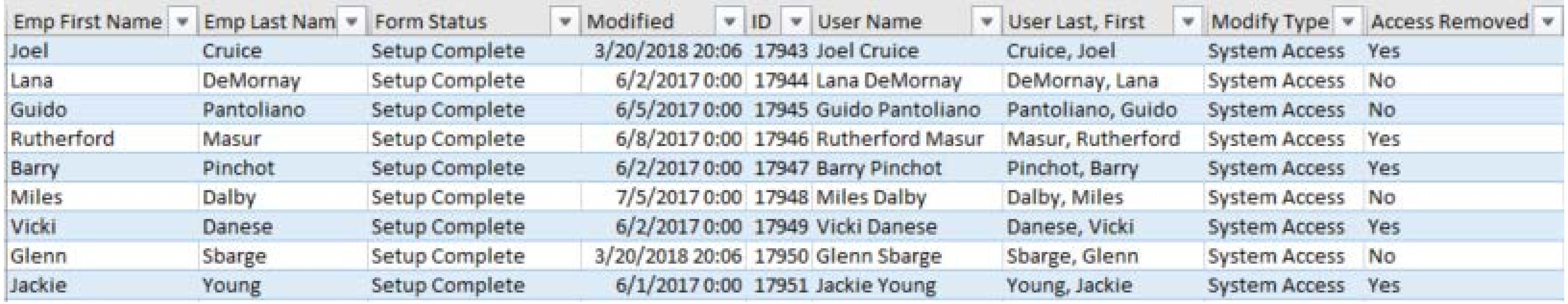
- Termination Action Date versus Termination Effective Date
- Include IT in termination process
- Define timeliness of disabling access
- Password change tracking
- Email Routing / Workflow queues
- Documenting date when account is disabled

Terminated Users

weaver
Assurance • Tax • Advisory



Emp ID	First Name	Middle Name	Last Name	Street Address	City/State/Zip	Hire Date	Termination Date
9740	Joel	T	Cruice	311 W Main St	Chicago IL 60652	09/17/2012	06/02/2017
9191	Lana	R	DeMornay	8848 E Tanque Verde Road	Chicago IL 60652	02/28/2006	06/02/2017
11216	Guido	J	Pantoliano	5201 Gulf Lane	Chicago IL 60652	08/15/2016	06/02/2017
9266	Rutherford	Richard	Masur	1719 243rd St	Chicago IL 60652	04/18/2011	06/02/2017
5139	Barry	B	Pinchot	9278 Royal Oak Lane	Chicago IL 60652	08/09/1999	06/02/2017
10268	Miles	Curtis	Dalby	2817 McCarthey Ave	Chicago IL 60652	08/04/2014	06/02/2017
11178	Vicki	Shera	Danese	2315 Norwich Court	Chicago IL 60652	08/15/2016	06/02/2017
11287	Glenn	R	Sbarge	112 Torrent Ave	Chicago IL 60652	09/06/2016	06/02/2017
11157	Jackie	Bruce	Young	1405 Jamaica Dr	Chicago IL 60652	01/08/2013	06/02/2017



Emp First Name	Emp Last Nam	Form Status	Modified	ID	User Name	User Last, First	Modify Type	Access Removed
Joel	Cruice	Setup Complete	3/20/2018 20:06	17943	Joel Cruice	Cruice, Joel	System Access	Yes
Lana	DeMornay	Setup Complete	6/2/2017 0:00	17944	Lana DeMornay	DeMornay, Lana	System Access	No
Guido	Pantoliano	Setup Complete	6/5/2017 0:00	17945	Guido Pantoliano	Pantoliano, Guido	System Access	No
Rutherford	Masur	Setup Complete	6/8/2017 0:00	17946	Rutherford Masur	Masur, Rutherford	System Access	Yes
Barry	Pinchot	Setup Complete	6/2/2017 0:00	17947	Barry Pinchot	Pinchot, Barry	System Access	Yes
Miles	Dalby	Setup Complete	7/5/2017 0:00	17948	Miles Dalby	Dalby, Miles	System Access	No
Vicki	Danese	Setup Complete	6/2/2017 0:00	17949	Vicki Danese	Danese, Vicki	System Access	Yes
Glenn	Sbarge	Setup Complete	3/20/2018 20:06	17950	Glenn Sbarge	Sbarge, Glenn	System Access	No
Jackie	Young	Setup Complete	6/1/2017 0:00	17951	Jackie Young	Young, Jackie	System Access	Yes

weaver
Assurance • Tax • Advisory

Change Management

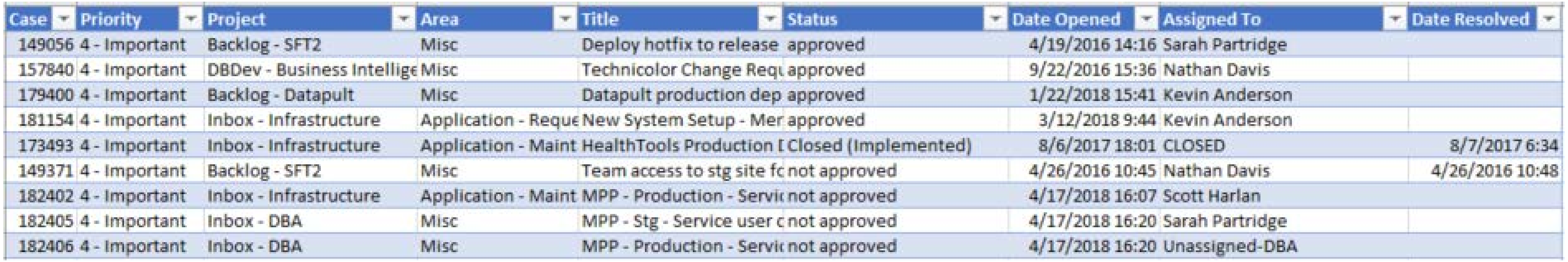
Change Management

- Not the change that was needed (though requested)
- Management signed off, but there was insufficient testing
- System becomes unavailable

Change Management

- Gather requirements
- Management authorization to develop
- User acceptance testing – documentation
- Regression testing
- Automated Testing
- Management approval to promote

Change Management



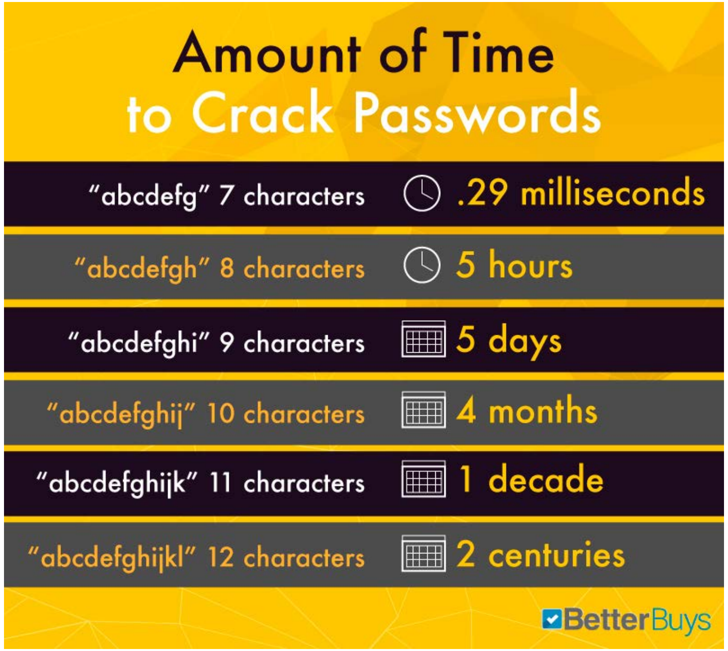
Case	Priority	Project	Area	Title	Status	Date Opened	Assigned To	Date Resolved
149056	4 - Important	Backlog - SFT2	Misc	Deploy hotfix to release	approved	4/19/2016 14:16	Sarah Partridge	
157840	4 - Important	DBDev - Business Intellige	Misc	Technicolor Change Requ	approved	9/22/2016 15:36	Nathan Davis	
179400	4 - Important	Backlog - Datapult	Misc	Datapult production dep	approved	1/22/2018 15:41	Kevin Anderson	
181154	4 - Important	Inbox - Infrastructure	Application - Reque	New System Setup - Mer	approved	3/12/2018 9:44	Kevin Anderson	
173493	4 - Important	Inbox - Infrastructure	Application - Maint	HealthTools Production [	Closed (Implemented)	8/6/2017 18:01	CLOSED	8/7/2017 6:34
149371	4 - Important	Backlog - SFT2	Misc	Team access to stg site fc	not approved	4/26/2016 10:45	Nathan Davis	4/26/2016 10:48
182402	4 - Important	Inbox - Infrastructure	Application - Maint	MPP - Production - Servi	not approved	4/17/2018 16:07	Scott Harlan	
182405	4 - Important	Inbox - DBA	Misc	MPP - Stg - Service user c	not approved	4/17/2018 16:20	Sarah Partridge	
182406	4 - Important	Inbox - DBA	Misc	MPP - Production - Servi	not approved	4/17/2018 16:20	Unassigned-DBA	

weaver
Assurance • Tax • Advisory

Passwords

Passwords

- Compromised passwords
  - Unauthorized access
  - Reliability of data
  - Sensitive/protected /confidential data is leaked



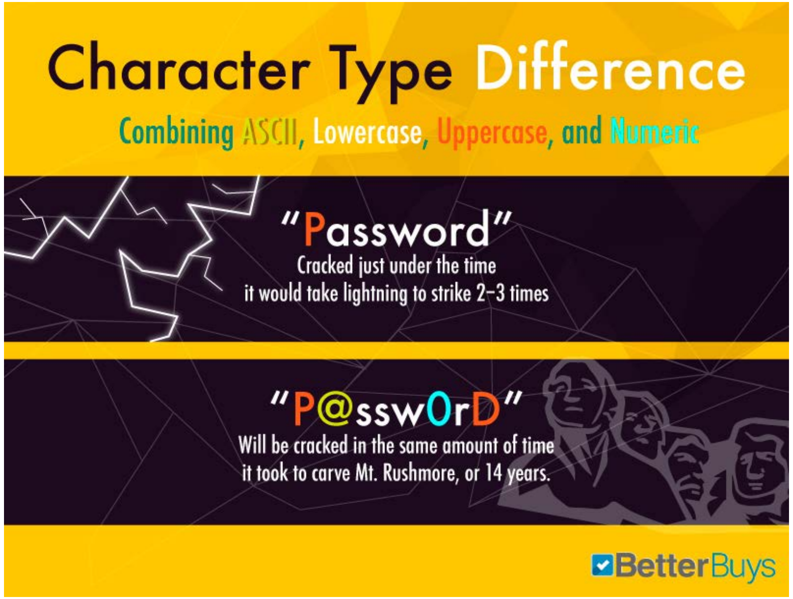
Amount of Time to Crack Passwords

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

BetterBuys

Passwords

- Minimum 8-characters
- Complex password- uppercase, lowercase, numbers, special characters
- Expires every 90 days
  - Minimum password age
- Password history of at least 5
- Account Lockout Threshold of 5
  - Counter Reset
  - Password Lockout Duration
- Initial password reset



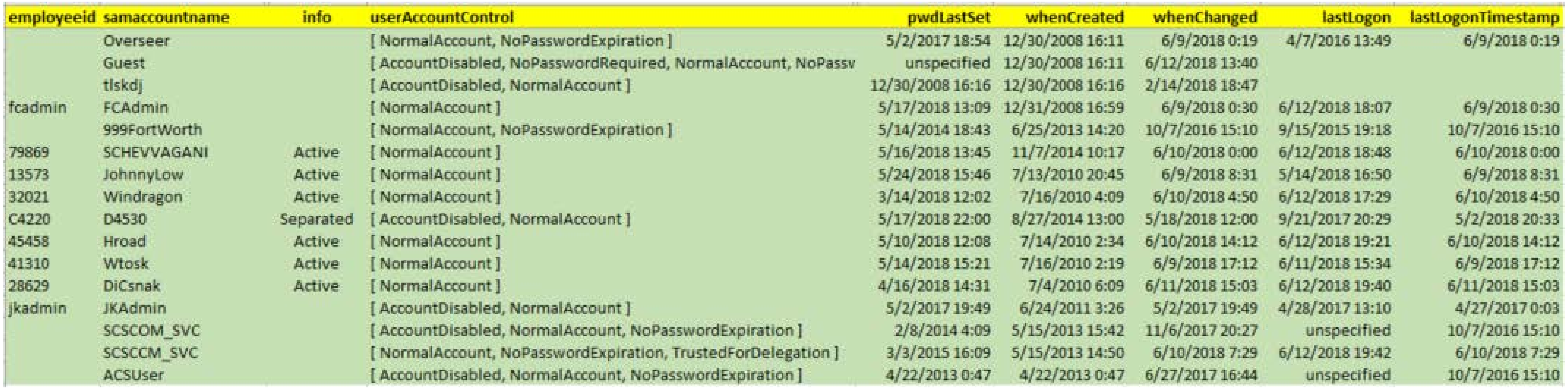
Character Type Difference

Combining ASCII, Lowercase, Uppercase, and Numeric

"Password"
Cracked just under the time
it would take lightning to strike 2-3 times

"P@sswOrD"
Will be cracked in the same amount of time
it took to carve Mt. Rushmore, or 14 years.

Passwords



employeeid	samaccountname	info	userAccountControl	pwdLastSet	whenCreated	whenChanged	lastLogon	lastLogonTimestamp
	Overseer		[NormalAccount, NoPasswordExpiration]	5/2/2017 18:54	12/30/2008 16:11	6/9/2018 0:19	4/7/2016 13:49	6/9/2018 0:19
	Guest		[AccountDisabled, NoPasswordRequired, NormalAccount, NoPassv	unspecified	12/30/2008 16:11	6/12/2018 13:40		
	tlskdj		[AccountDisabled, NormalAccount]	12/30/2008 16:16	12/30/2008 16:16	2/14/2018 18:47		
fcadmin	FCAdmin		[NormalAccount]	5/17/2018 13:09	12/31/2008 16:59	6/9/2018 0:30	6/12/2018 18:07	6/9/2018 0:30
	999FortWorth		[NormalAccount, NoPasswordExpiration]	5/14/2014 18:43	6/25/2013 14:20	10/7/2016 15:10	9/15/2015 19:18	10/7/2016 15:10
79869	SCHEVVAGANI	Active	[NormalAccount]	5/16/2018 13:45	11/7/2014 10:17	6/10/2018 0:00	6/12/2018 18:48	6/10/2018 0:00
13573	JohnnyLow	Active	[NormalAccount]	5/24/2018 15:46	7/13/2010 20:45	6/9/2018 8:31	5/14/2018 16:50	6/9/2018 8:31
32021	Windragon	Active	[NormalAccount]	3/14/2018 12:02	7/16/2010 4:09	6/10/2018 4:50	6/12/2018 17:29	6/10/2018 4:50
C4220	D4530	Separated	[AccountDisabled, NormalAccount]	5/17/2018 22:00	8/27/2014 13:00	5/18/2018 12:00	9/21/2017 20:29	5/2/2018 20:33
45458	Hroad	Active	[NormalAccount]	5/10/2018 12:08	7/14/2010 2:34	6/10/2018 14:12	6/12/2018 19:21	6/10/2018 14:12
41310	Wtosk	Active	[NormalAccount]	5/14/2018 15:21	7/16/2010 2:19	6/9/2018 17:12	6/11/2018 15:34	6/9/2018 17:12
28629	DiCsnak	Active	[NormalAccount]	4/16/2018 14:31	7/4/2010 6:09	6/11/2018 15:03	6/12/2018 19:40	6/11/2018 15:03
jkadmin	JKAdmin		[AccountDisabled, NormalAccount]	5/2/2017 19:49	6/24/2011 3:26	5/2/2017 19:49	4/28/2017 13:10	4/27/2017 0:03
	SCSCOM_SVC		[AccountDisabled, NormalAccount, NoPasswordExpiration]	2/8/2014 4:09	5/15/2013 15:42	11/6/2017 20:27	unspecified	10/7/2016 15:10
	SCSCCM_SVC		[NormalAccount, NoPasswordExpiration, TrustedForDelegation]	3/3/2015 16:09	5/15/2013 14:50	6/10/2018 7:29	6/12/2018 19:42	6/10/2018 7:29
	ACSUser		[AccountDisabled, NormalAccount, NoPasswordExpiration]	4/22/2013 0:47	4/22/2013 0:47	6/27/2017 16:44	unspecified	10/7/2016 15:10

Phishing

Phishing

- Spoofing email addresses to impersonate legitimate contacts

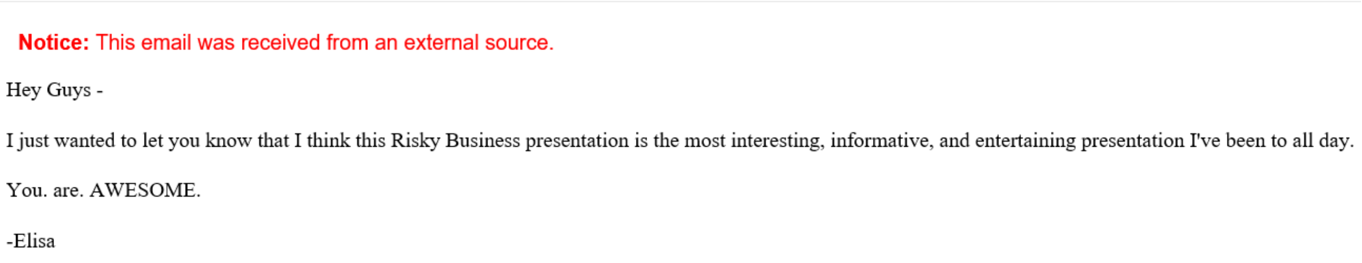
- Public reporting of payment registers = increased risk

Phishing

- Educate your organization on recognizing the signs
  - Security Awareness Training
  - Learning Modules
  - Breakroom Posters
  - Test Them!

Phishing

weaver
Assurance • Tax • Advisory



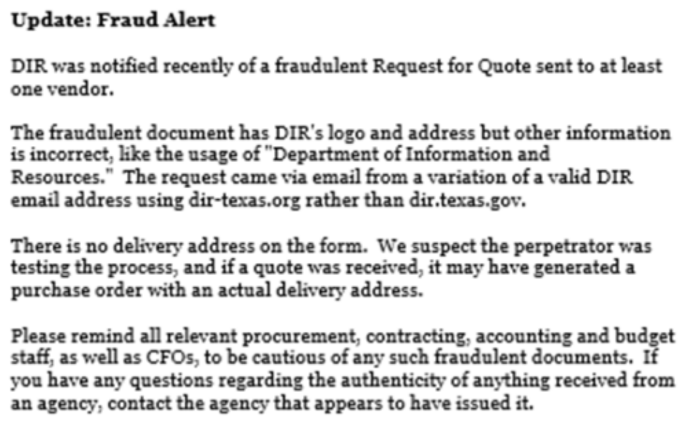
Notice: This email was received from an external source.

Hey Guys -

I just wanted to let you know that I think this Risky Business presentation is the most interesting, informative, and entertaining presentation I've been to all day.

You. are. AWESOME.

-Elisa



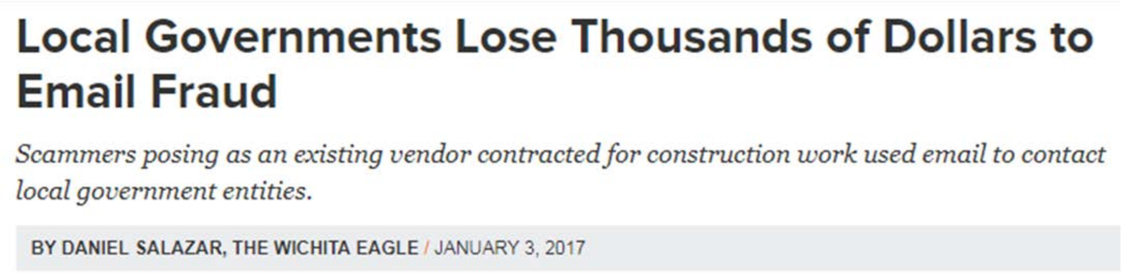
Update: Fraud Alert

DIR was notified recently of a fraudulent Request for Quote sent to at least one vendor.

The fraudulent document has DIR's logo and address but other information is incorrect, like the usage of "Department of Information and Resources." The request came via email from a variation of a valid DIR email address using dir-texas.org rather than dir.texas.gov.

There is no delivery address on the form. We suspect the perpetrator was testing the process, and if a quote was received, it may have generated a purchase order with an actual delivery address.

Please remind all relevant procurement, contracting, accounting and budget staff, as well as CFOs, to be cautious of any such fraudulent documents. If you have any questions regarding the authenticity of anything received from an agency, contact the agency that appears to have issued it.



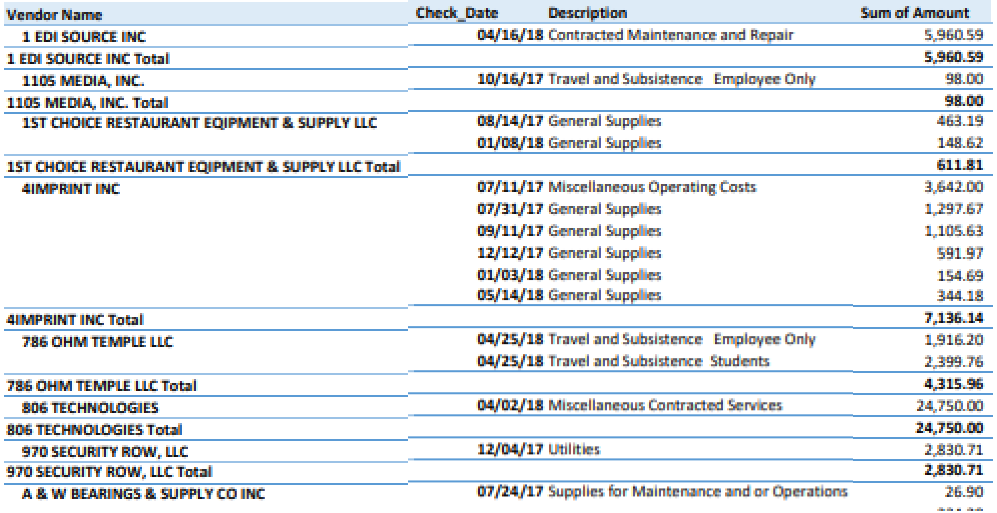
Local Governments Lose Thousands of Dollars to Email Fraud

Scammers posing as an existing vendor contracted for construction work used email to contact local government entities.

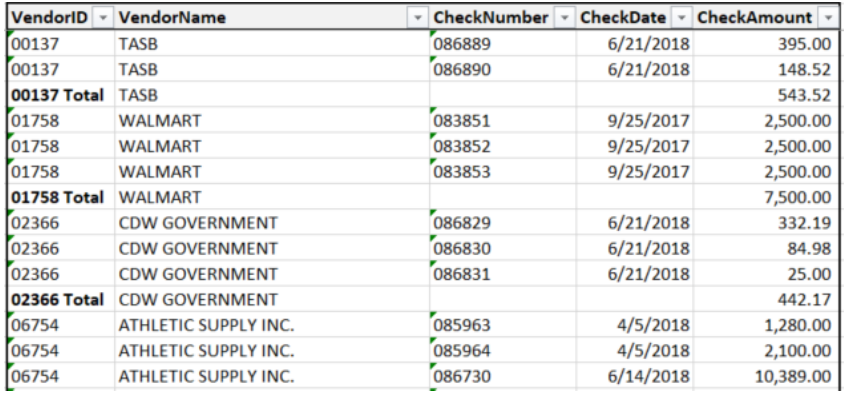
BY DANIEL SALAZAR, THE WICHITA EAGLE / JANUARY 3, 2017

Phishing

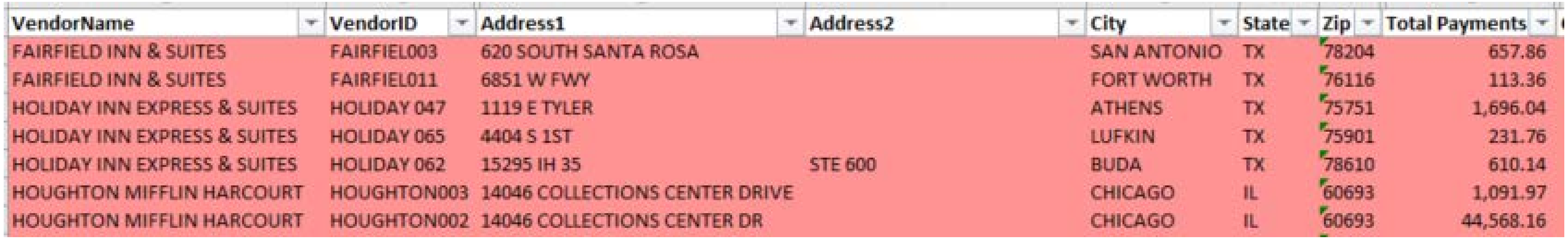
weaver
Assurance • Tax • Advisory



Vendor Name	Check_Date	Description	Sum of Amount
1 EDI SOURCE INC	04/16/18	Contracted Maintenance and Repair	5,960.59
1 EDI SOURCE INC Total			5,960.59
1105 MEDIA, INC.	10/16/17	Travel and Subsistence Employee Only	98.00
1105 MEDIA, INC. Total			98.00
1ST CHOICE RESTAURANT EQIPMENT & SUPPLY LLC	08/14/17	General Supplies	463.19
	01/08/18	General Supplies	148.62
1ST CHOICE RESTAURANT EQIPMENT & SUPPLY LLC Total			611.81
4IMPRINT INC	07/11/17	Miscellaneous Operating Costs	3,642.00
	07/31/17	General Supplies	1,297.67
	09/11/17	General Supplies	1,105.63
	12/12/17	General Supplies	591.97
	01/03/18	General Supplies	154.69
	05/14/18	General Supplies	344.18
4IMPRINT INC Total			7,136.14
786 OHM TEMPLE LLC	04/25/18	Travel and Subsistence Employee Only	1,916.20
	04/25/18	Travel and Subsistence Students	2,399.76
786 OHM TEMPLE LLC Total			4,315.96
806 TECHNOLOGIES	04/02/18	Miscellaneous Contracted Services	24,750.00
806 TECHNOLOGIES Total			24,750.00
970 SECURITY ROW, LLC	12/04/17	Utilities	2,830.71
970 SECURITY ROW, LLC Total			2,830.71
A & W BEARINGS & SUPPLY CO INC	07/24/17	Supplies for Maintenance and or Operations	26.90



VendorID	VendorName	CheckNumber	CheckDate	CheckAmount
00137	TASB	086889	6/21/2018	395.00
00137	TASB	086890	6/21/2018	148.52
00137 Total	TASB			543.52
01758	WALMART	083851	9/25/2017	2,500.00
01758	WALMART	083852	9/25/2017	2,500.00
01758	WALMART	083853	9/25/2017	2,500.00
01758 Total	WALMART			7,500.00
02366	CDW GOVERNMENT	086829	6/21/2018	332.19
02366	CDW GOVERNMENT	086830	6/21/2018	84.98
02366	CDW GOVERNMENT	086831	6/21/2018	25.00
02366 Total	CDW GOVERNMENT			442.17
06754	ATHLETIC SUPPLY INC.	085963	4/5/2018	1,280.00
06754	ATHLETIC SUPPLY INC.	085964	4/5/2018	2,100.00
06754	ATHLETIC SUPPLY INC.	086730	6/14/2018	10,389.00



VendorName	VendorID	Address1	Address2	City	State	Zip	Total Payments
FAIRFIELD INN & SUITES	FAIRFIEL003	620 SOUTH SANTA ROSA		SAN ANTONIO	TX	78204	657.86
FAIRFIELD INN & SUITES	FAIRFIEL011	6851 W FWY		FORT WORTH	TX	76116	113.36
HOLIDAY INN EXPRESS & SUITES	HOLIDAY 047	1119 E TYLER		ATHENS	TX	75751	1,696.04
HOLIDAY INN EXPRESS & SUITES	HOLIDAY 065	4404 S 1ST		LUFKIN	TX	75901	231.76
HOLIDAY INN EXPRESS & SUITES	HOLIDAY 062	15295 IH 35	STE 600	BUDA	TX	78610	610.14
HOUGHTON MIFFLIN HARCOURT	HOUGHTON003	14046 COLLECTIONS CENTER DRIVE		CHICAGO	IL	60693	1,091.97
HOUGHTON MIFFLIN HARCOURT	HOUGHTON002	14046 COLLECTIONS CENTER DR		CHICAGO	IL	60693	44,568.16

That’s all folks!

weaver
Assurance • Tax • Advisory

weaver
Assurance • Tax • Advisory

Questions?

Let’s Connect

@weavercpas

facebook.com/weavercpas

linkedin.com/company/weavercpas

youtube.com/weavercpas

Insights blog – weaver.com

Elisa Gilbertson, CPA
Manager, Weaver Analytics
Elisa.Gilbertson@weaver.com
832.320.7941

Raveen Bhasin, CISM, CISA, ITIL, CSM
Manager, IT Advisory Services
Raveen.Bhasin@weaver.com
972.448.9243