2019 SENATE INDUSTRY, BUSINESS AND LABOR

SB 2209

2019 SENATE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Roosevelt Park Room, State Capitol

SB 2209
1/21/2019
Job #31093

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Amy Crane

Explanation or reason for introduction of bill/resolution:

Relating to protection for records related to critical infrastructure and security planning, mitigation, or threats.

Minutes: Att. #1-2

Chairman Klein: Opened the hearing on SB 2209. All members were present.

Chairman Klein: I am one of the sponsors on this. I'm going to have Todd explain because in our discussions, he came to me and spoke a bit about what we need to do. This is from the Missouri River Energy Services which happens to be an energy company that sells electricity to some of the communities in my district and Senator Heckaman's.

Senator Joan Heckaman, District 23: Testified in support of the bill. I am a cosponsor on this bill. Specifically, because of the security risk that if we don't do this, may be imposed. But I'm going to take you back to the good old days in North Dakota when we had the party line phones, ours was three longs, some others were one short and two longs, four shorts for Senator Klein. And when the phone rang everybody ran to the phones to see who everybody was talking about. That's how information was conveyed and I'm not sure its much different these days because we don't know who's accessing our information now. And the reason I signed on to this bill is because of the possible threats to our infrastructure in North Dakota and along the lines that lead in to us and out of us. I wrote a comment to someone this weekend and said I believe its integral to all of our security across state agencies, schools, colleges, offices, infrastructure. We need to have a plan in the case of some kind of security breaches. And those plans, are no good if everyone can get to them and read them. Security means, just that, being secure. And I would not want my grandchildren to go schools where the building evacuation plan is an open record. Parents need that information, but can be obtained through their online accounts. So I believe anything that is really necessary, whether it's our infrastructure lines, or whether it's our personal lives or whatever, we need to have that secure. Cyber security threats are growing every day. I remember just a couple of years ago I was attending a leadership conference here in Bismarck, and the two Bismarck hospitals told us how many cyber-attacks they have every day. It was huge and actually scary that we don't know who's out there looking for information. If we can be secure in any of our plans across the state whether its schools, or infrastructure, with our power. I think its behooving of us to listen to this bill and see what we can do about this. All agencies are finding out that this is happening, all stakeholders across the state, no matter what kind of

industry you are in. Going forward we need to be sure that we are good stewards of the responsibilities that we have here in our state and be sure that we are keeping our information safe and secure.

Chairman Klein: My only comment would be times are different from the good old days. The questions are no longer if but when we get breached. There are people all over the world looking for information so it's best to be safe. Certainly today I wouldn't want them to turn the juice off, it might get a little cold in here.

Senator Heckaman: It's an important infrastructure here in North Dakota, whether it's utilities or whether it's any kind of other industry that we have. All of those are ripe for cyber-attacks and that information needs to be secure. If this is one way that can help us be secure in North Dakota and help our partner states too, then we need to do it.

(5:23)Todd Kranda, testifying on behalf of Deb Birgen, Missouri River Energy Services: See attachment #1 for testimony in support of the bill.

(11:28)Chairman Klein: We've worked on this a little while. Initially we had some resistance thinking we had this already in code. What we have here is a collaboration of what you wanted, counsel sees fit, and our consumers.

Todd: We started early enough, we had a number of clarifications, we had entities asked to be included. We made tweaks, got advice from legislative counsel. I haven't heard anyone being concerned with anything. I'm hopeful we can move this forward and get this accomplished.

Senator Burckhard: Do we have any other municipal electric communities in North Dakota or are these the only ones?

Todd: In terms of who the other communities might have, these are only our six members, so they are directly impacted by our services. We're stationed out of Sioux Falls, South Dakota is our home office and we operate in four other states. And municipal communities such as the six that I've listed are who contract with us to provide power to their municipalities. In terms of who else, I can get you a brochure of our region but I can't tell you what the other communities are doing.

Senator Piepkorn: Second page, number 4, line 18, how are you going to keep your contractors for construction, renovation, remodeling, probably local people. You know, to make sure that they are going to keep any information that they need, to complete their work, that they will also adhere to our confidentiality and security format?

Todd: The section that you're referring to is existing law, it's not underlined we're not changing anything. So how it's gone on in the past will continue.

Senator Piepkorn: Do you know then?

Todd: I'm not aware of what there is, I'm not aware that there's been a problem. What we're doing is enhancing the securities making sure that we're tightened up a little bit. That was

one of the first comments that we had from LC, is that this is already in law to some extent and we acknowledged that and our concept here was to further enhance the changing of the times, the situation that we think causes an update.

Chairman Klein: One question that was posed to me was did this come from the DAPL controversy? And I sent that on to you. And I know you have another bill in another committee. Will you answer that and comment on it?

Todd: The answer was very short. I sent the questions on to Deb Birgen, and the answer she sent back was pretty short and sweet, no it was not, absolutely not.

(16:37)Amy De Kok, Legal Counsel, North Dakota School Board Association: see attachment #2 for testimony in support of the bill.

(19:21)Senator Piepkorn: There's a lot of language in here that the district MAY develop, I'm talking about school districts in particular, may develop, it sounds like a lot of these steps are up to the district. Is there anything in the association requiring the schools to have an evacuation plan in case of an active shooter?

Amy: Our association is a resource and provides support so we don't regulate them in that we wouldn't require a sort of plan. But I believe every district has some sort of safety plan and it's up to the individual districts to determine what sort of items or specific procedures are required within the plan. The way code is written now, it focuses a lot on physical security and so these changes would allow some clarity that some of those threat assessment type of information can be exempt or confidential if they choose to do that.

Senator Piepkorn: So are the school boards in various districts, do you have an educational plan for them if they don't know much about cyber security? Anything you have in house to help them with that?

Amy: We do have a wealth of resources to direct them to, our association doesn't have the ability to provide them that training in house. But there are a number of resources for boards to access for that type of information.

Chairman Klein: You spoke about the education committee. Are they working on additional, cyber issues or is this, here we have an opportunity to jump on board, but what we've got is good stuff, but I heard some buts in there? Are we gonna be good just with this, it's a good start?

Amy: The senate education committee was working on a full safety plan bill that allowed districts to levy $5 mil for to develop school safety plans. Part of that bill, there was a discussion about amending section 44-04.24 for the very same type of purpose with the emphasis being on how school districts maintain that kind of information. This has a broader effect to other public entities and I think would essentially accomplish the same goal.

Jean Schafer, Senior Legislative Representative, Basin Electric: Testified in support of the bill. We have circulated the new drafts of this bill internally and vetted the language and felt very comfortable with what became the draft that you have before you today. We do

believe this holds the protections. We talked about things being on file with the public service commission for that, that would be citing of facilities and/or transmission. But there are also files that would be located with the department of emergency services. Anytime that they would have to be responding to anything, a lot of the things that we have out there are inherently a little dangerous. So having access and knowing exactly what is where, would be housed within that state department as well. So looking to protect the plans and information. As well as things like, what are our redundancies? So if we lose power, what's your redundant plan so you want to make sure you're protecting things like that. Hoping for a do pass.

Chairman Klein: Closed the hearing on SB 2209.

Senator Piepkorn: Move a Do Pass.

Senator Burckhard: Seconded.

A Roll Call Vote Was Taken: 6 yeas, 0 nays, 0 absent.

Motion carried.

Senator Piepkorn will carry the bill.

Date: 1/21
Roll Call Vote #: 1

2019 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 2209

Senate Industry, Business and Labor Committee

☐ Subcommittee

Amendment LC# or Description: _____

Recommendation: ☐ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Motion Made By Piepkorn Seconded By Burckhard

Senators	Yes	No	Senators	Yes	No
Chairman Klein	X		Senator Piepkorn	X	
Vice Chairman Vedaa	X				
Senator Burckhard	X				
Senator Kreun	X				
Senator Roers	X				

Total (Yes) 6 No 0

Absent 0

Floor Assignment Piepkorn

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2209: Industry, Business and Labor Committee (Sen. Klein, Chairman) recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2209 was placed on the Eleventh order on the calendar.

2019 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2209

2019 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Peace Garden Room, State Capitol

SB 2209
3/4/2019
33147

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Protection for records related to critical infrastructure and security planning, mitigation, or threats.

Minutes: Attachment 1, 2

Chairman Keiser: Opens the hearing on SB 2209.

Todd Kranda~Attorney at Kelsch Ruff Kranda Nagle & Ludwig Law Firm-Representing Missouri River Energy Services: Attachment 1.

8:00

Rep Schauer: What would you do to specifically to ward off a cyber-attack?

Todd Kranda: SB 2209 helps enhance the protection that ND already provides. It picks up some of the area to further share information protected. We will try to put more of a buffer to protect.

Rep Schauer: Who is the controlling authority to make it transparent.?

Todd Kranda: I guess that you do to determine what is open & not open. We are asking you to prepare to plug the gap that we see that exist & circulate the data amongst the various interested parties. No one appeared in the Senate to object to this process of maintain the transparency.

Rep P Anderson: Are you aware of where anyone has asked for these public records?

Todd Kranda: I'm not aware, we want to enhance the protection & a precautionary step.

Chairman Keiser: If there is an attempted breach, it has to be reported. With the passage, what & who is it reported, then keep it confidential.

Todd Kranda: I'm not sure of an answer. My best guess is yes. This is protecting the information.

Zac Smith~ND Association of Rural Electric Cooperatives: I agree with Mr Kranda & he did a great job presenting the issues.

Carlee MacLeod~President of the Utility Shareholders of North Dakota: We also support this bill & appreciate the work that Mr Kranda put into it.

Rep Louser: This bill sounded familiar. The GVA committee had a bill regarding cyber threats. Section 44-04-18, the state department of emergency services who receives reports. They are referencing chapter 37-17.1 if we could have our intern look at those two & seen this in this bill.

Chairman Keiser: They could receive them but we have to make sure they are required.

Rep Louser: I think we will find the answers in those two sections.

Chairman Keiser: Anyone else here to testify on SB 2209 in support, opposition, neutral?

Jack McDonald~ND Newscaster's Association: The only question I would have is, where people's records were taken & not told about it. The public needs to be informed that your records are taken. There should be some provision to be informed for the public. This bill seems to be the opposite.

Chairman Keiser: Closes the hearing.

Andrew Alexis Varvel~Self: Attachment 2. Testimony submitted.

2019 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Peace Garden Room, State Capitol

SB 2209
3/13/2019
33665

☐ Subcommittee
☐ Conference Committee

Committee Clerk: Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Protection for records related to critical infrastructure and security planning, mitigation, or threats.

Minutes: Attachment 1.

Chairman Keiser: Reopens the hearing on SB 2209. This bill is about protection for records related to critical infrastructure and security planning, mitigation, or threats.

Rep P Anderson: Attachment 1.

Chairman Keiser: Anyone have any concerns about SB 2209?

Rep P Anderson: (didn't turn on mike until later). Jack McDonald was concerned about on the confidentiality, if there is a breach are they required to let people know. This takes care of that concern.

Chairman Keiser: Did you review the amendment 19.0791.01001? Everyone ok with that?

Rep P Anderson: Move the adoption of the amendment.

Vice Chairman Lefor: Second.

Chairman Keiser: Further discussion?

Voice vote ~ motion carried.

Chairman Keiser: We have SB 2209 as amended before us, what are the wishes?

Rep P Anderson: Moves a Do Pass as Amended.

Rep D Ruby: Second.

Chairman Keiser: Further discussion?

Roll call was taken on SB 2209 for a Do Pass as Amended with 13 yes, 0 no, 1 absent & Rep P Anderson is the carrier.

DP 3/13/19

19.0791.01001
Title.02000

Prepared by the Legislative Council staff for
Senator Klein

March 4, 2019

PROPOSED AMENDMENTS TO SENATE BILL NO. 2209

Page 1, line 8, remove "required to be disclosed"

Page 1, line 9, replace "to another person for" with "regarding"

Page 2, after line 20, insert:

"5. Records deemed exempt under this section and disclosed to another entity continue to be exempt in the possession of the receiving entity."

Renumber accordingly

Date: Mar 13, 2019

Roll Call Vote #: 1

2019 HOUSE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. SB 2209

House Industry, Business and Labor **Committee**

☐ **Subcommittee**

Amendment LC# or Description: 19.0791.01001

Recommendation

☒ Adopt Amendment
☐ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions ☐ Reconsider ☐ _____

Motion Made by Rep Anderson **Seconded By** Rep Lefor

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser			Rep O'Brien		
Vice Chairman Lefor			Rep Richter		
Rep Bosch			Rep D Ruby		
Rep C Johnson			Rep Schauer		
Rep Kasper			Rep Adams		
Rep Laning			Rep P Anderson		
Rep Louser			Rep M Nelson		

Total (Yes) _____ No _____

Absent _____

Floor Assignment Voice vote- motion carried

Date: Mar 13, 2019

Roll Call Vote #: 2

2019 HOUSE STANDING COMMITTEE
ROLL CALL VOTES

BILL/RESOLUTION NO. SB 2209

House Industry, Business and Labor **Committee**

☐ **Subcommittee**

Amendment LC# or Description:

Recommendation

☐ Adopt Amendment
☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☒ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions ☐ Reconsider ☐

Motion Made by Rep Anderson **Seconded By** Rep Ruby

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser	X		Rep O'Brien	AB	
Vice Chairman Lefor	X		Rep Richter	X	
Rep Bosch	X		Rep D Ruby	X	
Rep C Johnson	X		Rep Schauer	X	
Rep Kasper	X		Rep Adams	X	
Rep Laning	X		Rep P Anderson	X	
Rep Louser	X		Rep M Nelson	X	

Total (Yes) 13 No 0

Absent 1

Floor Assignment Rep Anderson

REPORT OF STANDING COMMITTEE

SB 2209: Industry, Business and Labor Committee (Rep. Keiser, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (13 YEAS, 0 NAYS, 1 ABSENT AND NOT VOTING). SB 2209 was placed on the Sixth order on the calendar.

Page 1, line 8, remove "required to be disclosed"

Page 1, line 9, replace "to another person for" with "regarding"

Page 2, after line 20, insert:

"5. Records deemed exempt under this section and disclosed to another entity continue to be exempt in the possession of the receiving entity."

Renumber accordingly

2019 TESTIMONY

SB 2209

SB2209 1/21/19 Att #1 pg. 1

Testimony in Support of SENATE BILL 2209
Senate Industry Business and Labor Committee
January 21, 2019

Good morning, Chairman Klein, Members of the Senate Industry Business & Labor Committee, my name is Deb Birgen. Unfortunately, I am unable to attend today's hearing but I have asked Todd D. Kranda, an attorney at Kelsch Ruff Kranda Nagle & Ludwig law firm in Mandan and a lobbyist for Missouri River Energy Services, to appear on my behalf and provide this testimony in support of SB 2209. I serve as the Director of Legislative & Governmental Relations for Missouri River Energy Services (MRES). I am speaking to you on behalf of MRES which is a municipal power agency that provides wholesale electric power to six municipal electric communities in this state, including Cavalier, Hillsboro, Lakota, Northwood, Riverdale and Valley City.

MRES requested this bill to be introduced. The "why" behind SB 2209 actually started with discussions with members of the Iowa Utilities Board (IUB) about three years ago. The IUB staff were working more with utilities on cyber and physical security issues and encouraging collaboration on best practices. The IUB is a public entity subject to Iowa's open meetings and public records laws. As a result, the IUB decided to seek legislation clarifying that whenever the IUB received information from a utility or other entity concerning various aspects of cyber and physical security; such information would be exempt from open meetings/public records laws. After hearing of the possible IUB legislation, MRES worked with the IUB and legislators to make sure that such information was confidential not only at the IUB level, but at the city utility level as well. This confidentiality included security procedures, emergency preparedness, vulnerability assessments, emergency response protocols, etc. MRES was pleased that it was passed and signed by the Governor in 2017. MRES is subject to the open meetings and public records laws of all four states in which it operates: North Dakota, Iowa, Minnesota and South Dakota. Language similar to the Iowa law exists in South Dakota and Minnesota, and now MRES seeks similar language in North Dakota in SB 2209.

The point of SB 2209 is to first, expand the definition of cybersecurity and physical security to cover information and documentation as it pertains to fuel supply, vulnerability assessments,

evacuation plans, threat assessments, security plans, etc. Second, SB 2209 makes sure that such information in the possession of a municipal owned utility or any public entity remains confidential. Finally, SB 2209 makes sure that if utilities such as the investor-owned utilities, share such data with a North Dakota public entity, like the Public Service Commission, it remains confidential. This will allow the utilities in North Dakota and the Public Service Commission to share planning and assessment information that is relevant to electric service security, but otherwise would create grave vulnerabilities and potentially serious breaches if publically available.

Why is this important? Most of us have probably heard about the hacking of Ukrainian utilities in 2015. Hackers hijacked two distribution utilities in the Ukraine and cut power to more than 80,000 people. Fortunately, the utilities were able to get the systems back on line manually. Recently, a January 11, 2019, Wall Street Journal article discussed the 2018 cyberattack on a small 15-person company that works with utilities and government agencies, in a backdoor attempt to get at the electric grid. Anyone in the electric utility world will tell you that cyber-attacks are becoming a daily occurrence. Additionally, we need to worry about physical security. In 2013, there was a shooting attack on PG&E's Metcalf Transmission Substation in California, resulting in over $15M in equipment damage. Fortunately, the incident did not affect electric supply to customers, but demonstrates that utilities also need to protect information regarding access to and information about substations, distribution and transmission lines, operations centers, etc.

While MRES respects the need for transparency in state and local government, the stakes are just too high and the customer impact is just too precarious. As utilities collaborate with other entities to secure our grid, fuel supply and electric reliability, we need to make sure the information is kept confidential and does not inadvertently open an opportunity for a physical or cyber interruption. Access to information on assessing, planning and responding to such potential attacks could also open the door to serious vulnerabilities that utilities and their customers cannot have exposed. Therefore, on behalf of MRES I respectfully ask for a "**Do Pass**" recommendation on SB 2209.

Thank you for taking the time to consider these comments today and to consider the passage of SB 2209.

Wall Street Journal - Mon 1/21/19

SB2209
1/21/19
Att #1 pg. 3

- Some top White House aides cautioned Trump against declaring a national emergency to build a wall along the southern border and others cast about for alternatives to that goal, as the partial government shutdown continued. A1, A4
- The U.S. is moving ahead with plans to withdraw all its troops from Syria even though a rift with Turkey appears likely to delay the pullout, defense officials said. A1
- An extremist group seized control of most of Syria's last opposition stronghold, threatening a cease-fire intended to avert a Syrian military offensive. A6
- Pompeo spoke in Cairo to rally the Arab world against Iran, casting the Islamic Republic as the Trump administration's top concern in the region. A6
- Cohen will testify publicly before the House Oversight Committee, and its chairman said the panel would strive to avoid any conflict with Mueller's probe. A3
- U.S. negotiators said they pushed in trade talks for China to make reforms that would stop local firms from extracting technology from American rivals. A16
- Congo's Catholic Church denounced official presidential election results that resulted in opposition leader Tshisekedi being declared the winner. A8
- Maduro was sworn in to a second six-year term as Venezuela's president, in defiance of international calls for him to resign. A7

Cohen to Testify Before Panel

JEENAH MOON/REUTERS

Former Trump lawyer Michael Cohen will testify publicly before a House committee next month, one of several congressional appearances expected before his prison sentence is set to begin. A3

Russian Hack Exposes Weakness in U.S. Power Grid

Worst known system breach involved attacks on small contractors

By Rebecca Smith and Rob Barry

One morning in March 2017, Mike Vitello's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians. They were trying to hack into the power grid.

"They were intercepting my every email," Mr. Vitello says. "What the hell? I'm nobody."

"It's not you. It's who you know," says Ms. Cox.

The cyberattack on the 15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation's electric grid. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government.

A reconstruction of the hack reveals a glaring vulnerability at the heart of the country's electric system. Rather than strike the utilities head on, the hackers went after the system's unprotected underbelly—hundreds of contractors and subcontractors like All-Ways.

Please turn to page A9

Macy's Results Rain On Holiday Parade

By Sarah Nassauer

Macy's Inc. and other mall-based retailers said sales petered out at the end of the year as they continued to lose customers to discounters and e-commerce, highlighting how not all chains are positioned to benefit from a strong U.S. economy.

The year-end results—and a weak profit outlook from Macy's—clouded what have been upbeat expectations for the holiday sales season with consumers showing a hearty willingness to spend.

The news Thursday spooked investors, who sent shares of Macy's down nearly 18%, the department store's worst one-day decline on record. Rival Kohl's Corp. and mall stalwart L Brands Inc., the owner of Victoria's Secret, also posted tepid holiday sales, triggering a broader selloff in retail stocks.

"The holiday season began strong—particularly during Black Friday and the following Cyber Week, but weakened in the mid-December period," Macy's Chief Executive Jeff Gennette said.

The negative sentiment weighed on shares of discounters like Target Corp. and Costco Wholesale Corp.—and yet they have posted strong holiday sales. Those chains, which are less dependent on apparel, and Amazon.com Inc. have been taking market share from department stores. Target cited strong demand for toys and baby products along with seasonal gifts.

"The rising tide of retail sales hasn't floated all boats," said Neil Saunders, managing director of research firm GlobalData. "We are seeing a

Please turn to page A2

- Last-ditch bid for Sears tops $5 billion B3

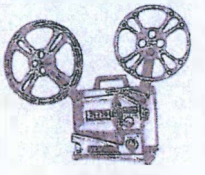
The Fans Are All That Move During Warhol's 8-Hour Film

Almost nothing happens in 'Empire,' except among those in the audience

By Brenda Cronin

Thomas Kiedrowski plans to bring a pillow to Saturday's screening of Andy Warhol's silent movie "Empire" in New York City.

While most agree the Warhol epic is a real snoozer, Mr. Kiedrowski is seeing it for the second time. The film runs eight hours, five minutes and consists of a single black-and-white shot of the Empire State Building.



Ten reels, zero plot

Spoiler alert: Not much happens beyond two things. Read on to find out.

"If it wasn't for the pillow, I don't know if I would be able to do it," said Mr. Kiedrowski, a 44-year-old librarian. He also plans to bring the same snacks that carried him through a 2010 showing—two yogurt smoothies and graham crackers to share with other die-hard fans of the late New York artist.

Mr. Kiedrowski, who wrote "Andy Warhol's New York City," might catch another "Empire" screening in March.

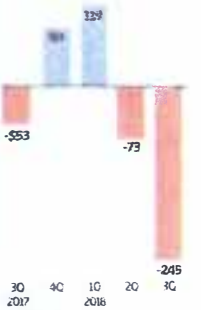
Since the film's 1965 debut, nearly all of the action has been off-screen.

Please turn to page A7

Downshift for Ford in Europe

Faced with losses in Europe, Ford Motor Co. is expected to overhaul its operations there, cutting thousands of jobs, closing plants and canceling low-profit models. B1

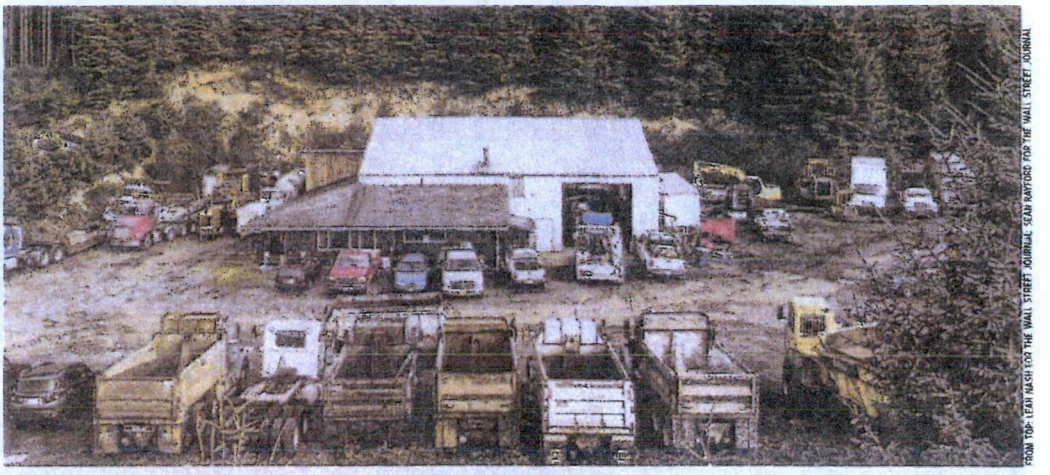
Ford Europe adjusted operating profit, in millions



Source: the company
THE WALL STREET JOURNAL

SB2209 1/21/19 Att #1 pg 4

Russia Hacked U.S. Grid



FROM TOP: LEAH NASH FOR THE WALL STREET JOURNAL; SEAN RAYFORD FOR THE WALL STREET JOURNAL

After breaching the network of Dan Kauffman Excavating in Oregon, top, hackers blasted out emails to roughly 2,300 of the company's contacts. Web developer Matt Hudson, above, says he had no idea Russians had hacked into his website, called imageliners.com.

Continued from Page One

who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.

The scheme's success came less from its technical prowess—though the attackers did use some clever tactics—than in how it exploited trusted business relationships using impersonation and trickery.

The hackers planted malware on sites of online publications frequently read by utility engineers. They sent out fake résumés with tainted attachments, pretending to be job seekers. Once they had computer-network credentials, they slipped through hidden portals used by utility technicians, in some cases getting into computer systems that monitor and control electricity flows.

The Wall Street Journal pieced together this account of how the attack unfolded through documents, computer records and interviews with people at the affected companies, current and former government officials and security-industry investigators.

The U.S. government hasn't named the utilities or other companies that were targeted. The Journal identified small businesses such as Commercial Contractors Inc. in Ridgefield, Wash., and Carlson Testing Inc., in Tigard, Ore., along with big utilities such as the federally owned Bonneville Power Administration and Berkshire Hathaway's PacifiCorp. Two of the energy companies targeted build systems that supply emergency power to Army bases.

The Russian campaign triggered an effort by the Federal Bureau of Investigation and Homeland Security to retrace the steps of the attackers and notify possible victims. Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

Early victims

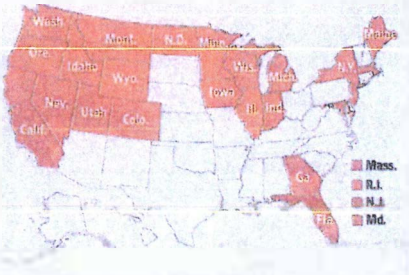
In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering."

The agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for

In the Crosshairs

Russian hackers seeking to infiltrate the power grid targeted companies operating in at least 24 states, Canada and the U.K.



Source: documents; interviews with people at the affected companies, government officials and security-industry investigators THE WALL STREET JOURNAL

and security experts who have reviewed the malicious code. That tactic enabled the Russians to gain access to ever more sensitive systems, said Homeland Security officials in industry briefings last year.

On March 2, 2017, the attackers used Mr. Vitello's account to send the mass email to customers, which was intended to herd recipients to a website secretly taken over by the hackers.

The email promised recipients that a document would download immediately, but nothing happened. Viewers were invited to click a link that said they could "download the file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month.

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also is possible the hackers used the site to open a back door into visitors' systems.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked

the email was fake.

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there, telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

Hacked site

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or

Drum is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power Corp., an independent power producer that sells electricity to more than a dozen utilities. In addition to downloading files from the site, the attackers visited the company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

"To our knowledge, there has never been a successful breach of any of the company's systems," Atlantic Power said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-person carpentry company in Michigan called DeVange Construction Inc. The emails appeared to come from an employee called Rick Harris—a persona fabricated by the attackers.

DeVange Construction's systems already may have been compromised. Applications to energy companies from nonexistent people seeking industrial-control systems jobs came from DeVange email addresses, according to security experts and emails reviewed by the Journal. Bogus résumés were attached—tweaked to trick recipients' computers into sending login information to hacked servers.

The Journal identified at least three utilities that received the emails: Washington-based Franklin PUD, Wisconsin-based Dairyland Power Cooperative and New York State Electric & Gas Corp. All three say they were aware of the hacking campaign but don't believe they fell victim to it.

A DeVange employee says federal agents visited the company. The company's owner, Jim Bell, declined to discuss the incident.

That June 30, the hackers sought remote access to an Indiana company that, like ReEnergy, installs equipment to allow government facilities to operate if the civilian grid loses power. That company, Energy Systems Group Ltd. of Newburgh, Ind., declines to say whether it was hacked.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Army officials said they take cybersecurity seriously but declined to comment further.

By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate networks, which are connected to the internet, and their critical-control networks, which are walled off from the web for security purposes. The bridges sometimes come in the form of "jump boxes," computers that give technicians a way to move between the two systems.

In briefings to utilities last summer, Jonathan Homer, industrial-control systems cybersecurity chief for Homeland Security, said the Russians had penetrated the control-system area of utilities through poorly protected jump boxes. The attackers had "legitimate access, the same as a technician," he said in one briefing, and could have temporarily knocked out power.

PacifiCorp says it wasn't compromised by any attack campaigns.

Gary Dodd, Bonneville's chief information security officer, says he doesn't believe his utility was breached. "It's possible something got in, but I really don't think so," he says.

The Army Corps says it doesn't comment on cybersecurity matters.

Going public

The U.S. government warned the public about the hacking campaign in an October 2017 advisory. It attributed it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility on "cyber actors" working for the Russian government, saying they had been active since at least March 2016.

Attackers exploited business relationships using impersonation and trickery.

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the

Short Circuit

SB 2209 1/21/19 Att #1 pg 5

government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

Early victims

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering."

The agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for Control Engineering. The agent warned it could be used to launch hostile actions against others.

Steve Rourke, CFE Media's co-founder, says his company took steps to fix the infected site. Before long, though, attackers laced other CFE Media trade publications with malicious content, according to security researchers at Accenture's iDefense unit and RiskIQ, a San Francisco cybersecurity company, who later analyzed the attack.

The hackers stalked visitors to these and other trade websites, hoping to catch engineers and others and penetrate the companies where they worked.

By planting a few lines of code on the websites, the attackers invisibly plucked computer usernames and passwords from unsuspecting visitors, according to government briefings on the attack file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month.

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also is possible the hackers used the site to open a back door into visitors' systems.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked the message.

All-Ways Excavating is a government contractor and bids for jobs with agencies including the U.S. Army Corps of Engineers, which operates dozens of federally owned hydroelectric facilities.

Some two weeks later, the attackers again used Mr. Vitello's account to send a barrage of emails.

One went to Dan Kauffman Excavating Inc, in Lincoln City, Ore., with the subject line. "Please DocuSign Signed Agreement—Funding Project."

Office manager Corinna Sawyer thought the wording was strange and emailed Mr. Vitello: "Just received this from your email, I assume you have been hacked."

Back came a response from the intruders who controlled Mr. Vitello's account: "I did send it."

Ms. Sawyer, still suspicious, called Mr. Vitello, who told her

Source: documents; interviews with people at the affected companies, government officials and security-industry investigators THE WALL STREET JOURNAL.

the email was fake.

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

Hacked site

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or catch it," says the company's owner.

In June 2017, the hackers used the Corvallis company's systems to go hunting. Over the next month, they accessed the Oregon company's network dozens of times, targeting at least six energy firms.

In some cases, the attackers simply studied the new targets' websites, possibly as reconnaissance for future strikes. In other instances, they may have gained footholds inside their victims' systems.

Two of the targeted companies had helped the Army create independent supplies of electricity for domestic bases.

On June 15, hackers visited the website of ReEnergy Holdings LLC. The renewable-energy company had built a small power plant that allows Fort Drum in western New York to operate even if the civilian power grid collapses. Fort Drum is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power Corp., an independent power producer that sells electricity to more than a dozen utilities. In addition to downloading files from the site, the attackers visited the company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

"To our knowledge, there has never been a successful breach of any of the company's systems," Atlantic Power said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-per- loses power. That company, Energy Systems Group Ltd. of Newburgh, Ind., declines to say whether it was hacked.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Army officials said they take cybersecurity seriously but declined to comment further.

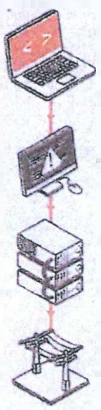
By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate

Short Circuit

Russian hackers targeted utilities' control-system computers.



Hacker

Russian hackers use malicious emails to steal credentials from utility company employees.

Employee computer

Using stolen credentials, hackers remotely access power-utility workstations and run malicious code.

Scada server

From the compromised workstation, hackers can gain access to the utility's supervisory control and data acquisition system (Scada).

Electrical equipment

Scada controls utility assets, including substations and power-generation facilities.

Sources: Department of Homeland Security (hacking); Department of Energy (Scada network) THE WALL STREET JOURNAL.

it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility on "cyber actors" working for the Russian government, saying they had been active since at least March 2016.

Attackers exploited business relationships using impersonation and trickery.

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the Bonneville Power Administration.

Vikram Thakur, technical director of security response for Symantec Corp., a California-based cybersecurity firm, says his company knows from its utility clients and from other security firms it works with that at least 60 utilities were targeted, including some outside the U.S. About two dozen were breached, he says, adding that hackers penetrated far enough to reach the industrial-control systems at eight or more utilities. He declined to name them.

The government isn't sure how many utilities and vendors in all were compromised in the Russian assault.

Industry experts say Russian government hackers likely remain inside some systems, undetected and awaiting further orders.

—*Lisa Schwartz contributed to this article.*

NDSBA
NORTH DAKOTA SCHOOL BOARDS ASSOCIATION
P.O. Box 7128
Bismarck ND 58507-7128
1-800-932-8791 • (701)255-4127
www.ndsba.org

TESTIMONY ON SB 2209
SENATE INDUSTRY, BUSINESS AND LABOR COMMITTEE
January 21, 2019
By Amy L. De Kok, Legal Counsel
North Dakota School Boards Association

Chairman and Members of the Committee:

My name is Amy De Kok and I am in-house Legal Counsel for the North Dakota School Boards Association (NDSBA). NDSBA represents all operating schools districts within the State of North Dakota. I appear before you today to testify in support of SB 2209.

Currently, section 44-04-24 of the NDCC only exempts "security systems" from open records requests. This exemption was created in 2003 following 9/11. While we believe the intent was to restrict highly sensitive information including evacuation plans, emergency response plans and other security measures, the language adopted places a strong emphasis on physical and electronic security. The ability to restrict disclosure of this type of information to the general public is still necessary; however, the safety planning and associated procedures that a public entity, particularly school districts, must develop are much broader today. Our members serve arguably the most vulnerable population of North Dakotans and are entrusted with their safety and health. It is important that districts have the ability to keep information and records related to threat response and assessments, as well as emergency evacuation procedures, closed in certain circumstances. For example: a district may develop an active shooter response or evacuation plan. A publicly available evacuation plan would make students sitting ducks.

We believe the amendments proposed by SB 2209 further clarify the ability of a public entity to keep information relating to threat assessments, threat response plans, and emergency evacuation plans closed when necessary. I'd be happy to answer any questions you have regarding the position taken by NDSBA on SB 2209. Thank you.

Attachment 1

Testimony in Support of
SENATE BILL 2209
House Industry Business and Labor Committee
March 4, 2019

Good morning, Chairman Keiser, Members of the House Industry Business & Labor Committee, my name is Deb Birgen. Unfortunately, I am unable to attend today's hearing but I have asked Todd D. Kranda, an attorney at Kelsch Ruff Kranda Nagle & Ludwig law firm in Mandan and a lobbyist for Missouri River Energy Services, to appear on my behalf and provide this testimony in support of SB 2209. I serve as the Director of Legislative & Governmental Relations for Missouri River Energy Services (MRES). I am speaking to you on behalf of MRES which is a municipal power agency that provides wholesale electric power to six municipal electric communities in this state, including Cavalier, Hillsboro, Lakota, Northwood, Riverdale and Valley City.

MRES requested this bill to be introduced. The "why" behind SB 2209 actually started with discussions with members of the Iowa Utilities Board (IUB) about three years ago. The IUB staff were working more with utilities on cyber and physical security issues and encouraging collaboration on best practices. The IUB is a public entity subject to Iowa's open meetings and public records laws. As a result, the IUB decided to seek legislation clarifying that whenever the IUB received information from a utility or other entity concerning various aspects of cyber and physical security; such information would be exempt from open meetings/public records laws. After hearing of the possible IUB legislation, MRES worked with the IUB and legislators to make sure that such information was confidential not only at the IUB level, but at the city utility level as well. This confidentiality included security procedures, emergency preparedness, vulnerability assessments, emergency response protocols, etc. MRES was pleased that it was passed and signed by the Governor in 2017. MRES is subject to the open meetings and public records laws of all four states in which it operates: North Dakota, Iowa, Minnesota and South Dakota. Language similar to the Iowa law exists in South Dakota and Minnesota, and now MRES seeks similar language in North Dakota in SB 2209.

The point of SB 2209 is to first, expand the definition of cybersecurity and physical security to cover information and documentation as it pertains to fuel supply, vulnerability assessments, evacuation plans, threat assessments, security plans, etc. Second, SB 2209 makes sure that such information in the possession of a municipal owned utility or any public entity remains confidential. Finally, SB 2209 makes sure that if utilities such as the investor-owned utilities, share such data with a North Dakota public entity, like the Public Service Commission, it remains confidential. This will allow the utilities in North Dakota and the Public Service

Commission to share planning and assessment information that is relevant to electric service security, but otherwise would create grave vulnerabilities and potentially serious breaches if publically available.

Why is this important? Most of us have probably heard about the hacking of Ukrainian utilities in 2015. Hackers hijacked two distribution utilities in the Ukraine and cut power to more than 80,000 people. Fortunately, the utilities were able to get the systems back on line manually. Recently, a January 11, 2019, Wall Street Journal article discussed the 2018 cyberattack on a small 15-person company that works with utilities and government agencies, in a backdoor attempt to get at the electric grid. Anyone in the electric utility world will tell you that cyber-attacks are becoming a daily occurrence. Additionally, we need to worry about physical security. In 2013, there was a shooting attack on PG&E's Metcalf Transmission Substation in California, resulting in over $15M in equipment damage. Fortunately, the incident did not affect electric supply to customers, but demonstrates that utilities also need to protect information regarding access to and information about substations, distribution and transmission lines, operations centers, etc.

I will note that we were contacted last week by the North Dakota Attorney General's Office regarding a tweak they believe is needed in the bill. After discussing this with the Attorney General's office, I concur that they are correct in the needed language update. An amendment is being drafted by the Legislative Council. In the amendment, we would ask that the phrase "required to be disclosed to another person" be removed from page one, lines 8-9. Then we'd request a new subsection—subsection 5 be added at or after line 20, page two to say "Records disclosed to another entity continue to be exempt in the possession of the receiving entity." Although this means the bill would need to go back to the Senate for a concurring vote, we agree with the Attorney General's Office that this amendment is necessary to avoid any inadvertent misinterpretation.

While MRES respects the need for transparency in state and local government, the stakes are just too high and the customer impact is just too precarious. As utilities collaborate with other entities to secure our grid, fuel supply and electric reliability, we need to make sure the information is kept confidential and does not inadvertently open an opportunity for a physical or cyber interruption. Access to information on assessing, planning and responding to such potential attacks could also open the door to serious vulnerabilities that utilities and their customers cannot have exposed. Therefore, on behalf of MRES I respectfully ask for a "**Do Pass**" recommendation on SB 2209.

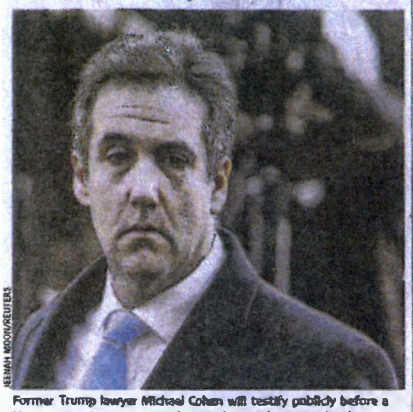
Thank you for taking the time to consider these comments today and to consider the passage of SB 2209.

Mar 4, 2019 SB 2209 Attachment 1

Wall Street Journal - 3/1/19

- **Some top White House aides cautioned** Trump against declaring a national emergency to build a wall along the southern border and others cast about for alternatives to that goal, as the partial government shutdown continued. A1, A4
- **The U.S. is moving ahead** with plans to withdraw all its troops from Syria even though a rift with Turkey appears likely to delay the pullout, defense officials said. A1
- **An extremist group** seized control of most of Syria's last opposition stronghold, threatening a cease-fire intended to avert a Syrian military offensive. A6
- **Pompeo spoke** in Cairo to rally the Arab world against Iran, casting the Islamic Republic as the Trump administration's top concern in the region. A6
- **Cohen will testify** publicly before the House Oversight Committee, and its chairman said the panel would strive to avoid any conflict with Mueller's probe. A3
- **U.S. negotiators said** they pushed in trade talks for China to make reforms that would stop local firms from extracting technology from American rivals. A16
- **Congo's Catholic Church** denounced official presidential election results that resulted in opposition leader Tshisekedi being declared the winner. A8
- **Maduro was sworn in** to a second six-year term as Venezuela's president, in defiance of international calls for him to resign. A7

Cohen to Testify Before Panel



KEVIN MOOG/REUTERS

Former Trump lawyer Michael Cohen will testify publicly before a House committee next month, one of several congressional appearances expected before his prison sentence is set to begin. A3

Russian Hack Exposes Weakness in U.S. Power Grid

Worst known system breach involved attacks on small contractors

By Rebecca Smith and Rob Barry

One morning in March 2017, Mike Vitello's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians. They were trying to hack into the power grid.

"They were intercepting my every email," Mr. Vitello says. "What the hell? I'm nobody."

"It's not you. It's who you know," says Ms. Cox.

The cyberattack on the 15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation's electric grid. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government.

A reconstruction of the hack reveals a glaring vulnerability at the heart of the country's electric system. Rather than strike the utilities head on, the hackers went after the system's unprotected underbelly—hundreds of contractors and subcontractors like All-Ways.

Please turn to page A9

Macy's Results Rain On Holiday Parade

By Sarah Nassauer

Macy's Inc. and other mall-based retailers said sales petered out at the end of the year as they continued to lose customers to discounters and e-commerce, highlighting how not all chains are positioned to benefit from a strong U.S. economy.

The year-end results—and a weak profit outlook from Macy's—clouded what have been upbeat expectations for the holiday sales season with consumers showing a hearty willingness to spend.

The news Thursday spooked investors, who sent shares of Macy's down nearly 18%, the department store's worst one-day decline on record. Rival Kohl's Corp. and mall stalwart L Brands Inc., the owner of Victoria's Secret, also posted tepid holiday sales, triggering a broader selloff in retail stocks.

"The holiday season began strong—particularly during Black Friday and the following Cyber Week, but weakened in the mid-December period," Macy's Chief Executive Jeff Gennette said.

The negative sentiment weighed on shares of discounters like Target Corp. and Costco Wholesale Corp.—and yet they have posted strong holiday sales. Those chains, which are less dependent on apparel, and Amazon.com Inc. have been taking market share from department stores. Target cited strong demand for toys and baby products along with seasonal gifts.

"The rising tide of retail sales hasn't floated all boats," said Neil Saunders, managing director of research firm GlobalData. "We are seeing a

Please turn to page A2

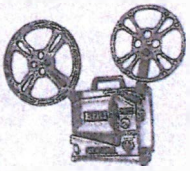
The Fans Are All That Move During Warhol's 8-Hour Film

Almost nothing happens in 'Empire,' except among those in the audience

By Brenda Cronin

Thomas Kiedrowski plans to bring a pillow to Saturday's screening of Andy Warhol's silent movie "Empire" in New York City.

While most agree the Warhol epic is a real snoozer, Mr. Kiedrowski is seeing it for the second time. The film runs eight hours, five minutes and consists of a single black-and-white shot of the Empire State Building.



Ten reels, zero plot

Spoiler alert: Not much happens beyond two things. Read on to find out.

"If it wasn't for the pillow, I don't know if I would be able to do it," said Mr. Kiedrowski, a 44-year-old librarian. He also plans to bring the same snacks that carried him through a 2010 showing—two yogurt smoothies and graham crackers to share with other die-hard fans of the late New York artist.

Mr. Kiedrowski, who wrote "Andy Warhol's New York City," might catch another "Empire" screening in March.

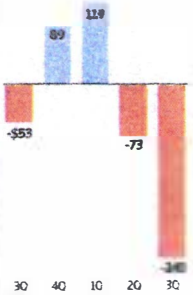
Since the film's 1965 debut, nearly all of the action has been off-screen.

Please turn to page A7

Downshift for Ford in Europe

Faced with losses in Europe, Ford Motor Co. is expected to overhaul its operations there, cutting thousands of jobs, closing plants and canceling low-profit models. B1

Ford Europe adjusted operating profit, in millions



Source: the company

THE WALL STREET JOURNAL.

3

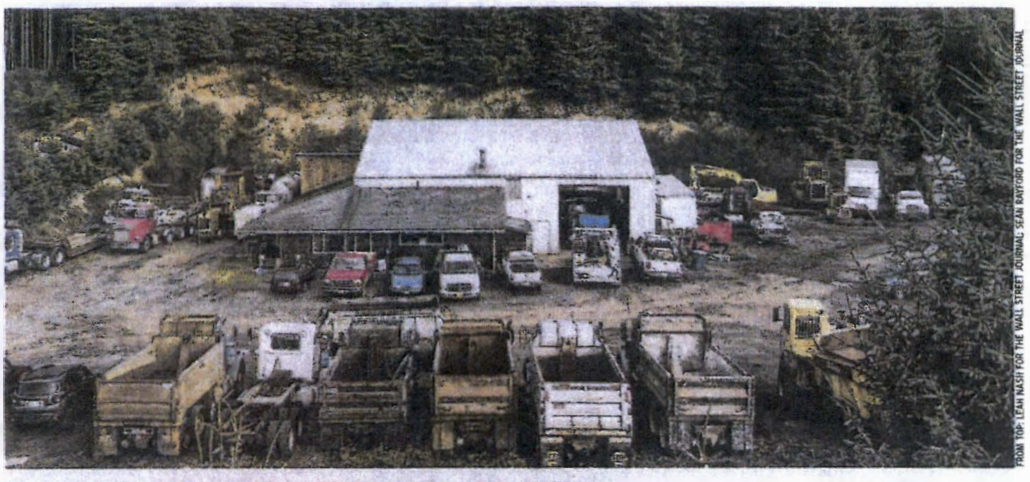
SB 2209

Mar 4, 2019

FROM PAGE ONE

Attachment 1

Russia Hacked U.S. Grid



FROM TOP: LEAH NASH FOR THE WALL STREET JOURNAL; SEAN RAYFORD FOR THE WALL STREET JOURNAL

After breaching the network of Dan Kauffman Excavating in Oregon, top, hackers blasted out emails to roughly 2,300 of the company's contacts. Web developer Matt Hudson, above, says he had no idea Russians had hacked into his website, called imageliners.com.

Continued from Page One

who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.

The scheme's success came less from its technical prowess—though the attackers did use some clever tactics—than in how it exploited trusted business relationships using impersonation and trickery.

The hackers planted malware on sites of online publications frequently read by utility engineers. They sent out fake résumés with tainted attachments, pretending to be job seekers. Once they had computer-network credentials, they slipped through hidden portals used by utility technicians, in some cases getting into computer systems that monitor and control electricity flows.

The Wall Street Journal pieced together this account of how the attack unfolded through documents, computer records and interviews with people at the affected companies, current and former government officials and security-industry investigators.

The U.S. government hasn't named the utilities or other companies that were targeted. The Journal identified small businesses such as Commercial Contractors Inc. in Ridgefield, Wash., and Carlson Testing Inc., in Tigard, Ore., along with big utilities such as the federally owned Bonneville Power Administration and Berkshire Hathaway's PacifiCorp. Two of the energy companies targeted build systems that supply emergency power to Army bases.

The Russian campaign triggered an effort by the Federal Bureau of Investigation and Homeland Security to retrace the steps of the attackers and notify possible victims. Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

Early victims

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering."

The agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for

and security experts who have reviewed the malicious code. That tactic enabled the Russians to gain access to ever more sensitive systems, said Homeland Security officials in industry briefings last year.

On March 2, 2017, the attackers used Mr. Vitello's account to send the mass email to customers, which was intended to herd recipients to a website secretly taken over by the hackers.

The email promised recipients that a document would download immediately, but nothing happened. Viewers were invited to click a link that said they could "download the file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

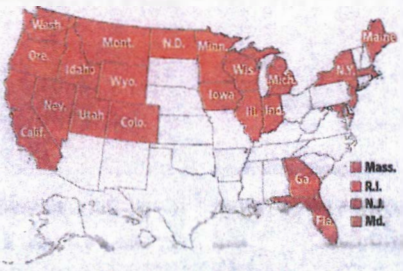
The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month.

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also is possible the hackers used the site to open a back door into visitors' systems.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked

In the Crosshairs

Russian hackers seeking to infiltrate the power grid targeted companies operating in at least 24 states, Canada and the U.K.



Source: documents; interviews with people at the affected companies, government officials and security-industry investigators THE WALL STREET JOURNAL.

the email was fake.

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there, telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

Hacked site

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or

Drum is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power Corp., an independent power producer that sells electricity to more than a dozen utilities. In addition to downloading files from the site, the attackers visited the company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

"To our knowledge, there has never been a successful breach of any of the company's systems," Atlantic Power said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-person carpentry company in Michigan called DeVange Construction Inc. The emails appeared to come from an employee called Rick Harris—a persona fabricated by the attackers.

DeVange Construction's systems already may have been compromised. Applications to energy companies from nonexistent people seeking industrial-control systems jobs came from DeVange email addresses, according to security experts and emails reviewed by the Journal. Bogus résumés were attached—tweaked to trick recipients' computers into sending login information to hacked servers.

The Journal identified at least three utilities that received the emails: Washington-based Franklin PUD, Wisconsin-based Dairyland Power Cooperative and New York State Electric & Gas Corp. All three say they were aware of the hacking campaign but don't believe they fell victim to it.

A DeVange employee says federal agents visited the company. The company's owner, Jim Bell, declined to discuss the incident.

That June 30, the hackers sought remote access to an Indiana company that, like ReEnergy, installs equipment to allow government facilities to operate if the civilian grid loses power. That company, Energy Systems Group Ltd. of Newburgh, Ind., declines to say whether it was hacked.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Army officials said they take cybersecurity seriously but declined to comment further.

By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate networks, which are connected to the internet, and their critical-control networks, which are walled off from the web for security purposes. The bridges sometimes come in the form of "jump boxes," computers that give technicians a way to move between the two systems.

In briefings to utilities last summer, Jonathan Homer, industrial-control systems cybersecurity chief for Homeland Security, said the Russians had penetrated the control-system area of utilities through poorly protected jump boxes. The attackers had "legitimate access, the same as a technician," he said in one briefing, and could have temporarily knocked out power.

PacifiCorp says it wasn't compromised by any attack campaigns.

Gary Dodd, Bonneville's chief information security officer, says he doesn't believe his utility was breached. "It's possible something got in, but I really don't think so," he says.

The Army Corps says it doesn't comment on cybersecurity matters.

Going public

The U.S. government warned the public about the hacking campaign in an October 2017 advisory. It attributed it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility on "cyber actors" working for the Russian government, saying they had been active since at least March 2016.

Attackers exploited business relationships using impersonation and trickery.

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the Bonneville Power Administra-

Short Circuit

4

government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

Early victims

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering."

The agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for Control Engineering. The agent warned it could be used to launch hostile actions against others.

Steve Rourke, CFE Media's co-founder, says his company took steps to fix the infected site. Before long, though, attackers laced other CFE Media trade publications with malicious content, according to security researchers at Accenture's iDefense unit and RiskIQ, a San Francisco cybersecurity company, who later analyzed the attack.

The hackers stalked visitors to these and other trade websites, hoping to catch engineers and others and penetrate the companies where they worked.

By planting a few lines of code on the websites, the attackers invisibly plucked computer usernames and passwords from unsuspecting visitors, according to government briefings on the attack file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month.

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also is possible the hackers used the site to open a back door into visitors' systems.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked the message.

All-Ways Excavating is a government contractor and bids for jobs with agencies including the U.S. Army Corps of Engineers, which operates dozens of federally owned hydroelectric facilities.

Some two weeks later, the attackers again used Mr. Vitello's account to send a barrage of emails.

One went to Dan Kauffman Excavating Inc., in Lincoln City, Ore., with the subject line: "Please DocuSign Signed Agreement—Funding Project."

Office manager Corinna Sawyer thought the wording was strange and emailed Mr. Vitello: "Just received this from your email, I assume you have been hacked."

Back came a response from the intruders who controlled Mr. Vitello's account: "I did send it."

Ms. Sawyer, still suspicious, called Mr. Vitello, who told her

Source: documents; interviews with people at the affected companies, government officials and security-industry investigators THE WALL STREET JOURNAL.

the email was fake.

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there, telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

Hacked site

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or catch it," says the company's owner.

In June 2017, the hackers used the Corvallis company's systems to go hunting. Over the next month, they accessed the Oregon company's network dozens of times, targeting at least six energy firms.

In some cases, the attackers simply studied the new targets' websites, possibly as reconnaissance for future strikes. In other instances, they may have gained footholds inside their victims' systems.

Two of the targeted companies had helped the Army create independent supplies of electricity for domestic bases.

On June 15, hackers visited the website of ReEnergy Holdings LLC. The renewable-energy company had built a small power plant that allows Fort Drum in western New York to operate even if the civilian power grid collapses. Fort Drum is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power Corp., an independent power producer that sells electricity to more than a dozen utilities. In addition to downloading files from the site, the attackers visited the company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

"To our knowledge, there has never been a successful breach of any of the company's systems," Atlantic Power said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-person power. That company, Energy Systems Group Ltd. of Newburgh, Ind., declines to say whether it was hacked.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Army officials said they take cybersecurity seriously but declined to comment further.

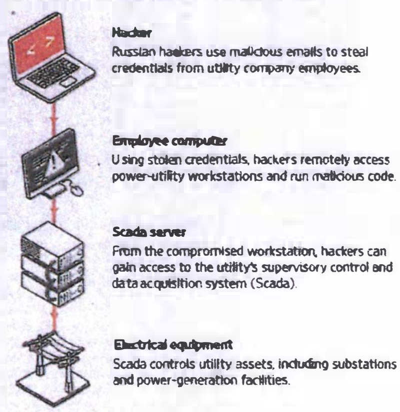
By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate

Short Circuit

Russian hackers targeted utilities' control-system computers.



Sources: Department of Homeland Security (hacking); Department of Energy (Scada network) THE WALL STREET JOURNAL.

it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility on "cyber actors" working for the Russian government, saying they had been active since at least March 2016.

Attackers exploited business relationships using impersonation and trickery.

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the Bonneville Power Administration.

Vikram Thakur, technical director of security response for Symantec Corp., a California-based cybersecurity firm, says his company knows from its utility clients and from other security firms it works with that at least 60 utilities were targeted, including some outside the U.S. About two dozen were breached, he says, adding that hackers penetrated far enough to reach the industrial-control systems at eight or more utilities. He declined to name them.

The government isn't sure how many utilities and vendors in all were compromised in the Russian assault.

Industry experts say Russian government hackers likely remain inside some systems, undetected and awaiting further orders.

—Lisa Schwartz contributed to this article.

Mar 4, 2019 SB 2209 Attachment 1

Attachment 1

19.0791.01001
Title.

Prepared by the Legislative Council staff for
Senator Klein

March 4, 2019

PROPOSED AMENDMENTS TO SENATE BILL NO. 2209

Page 1, line 8, remove "required to be disclosed"

Page 1, line 9, replace "to another person for" with "regarding"

Page 2, after line 20, insert:

"5. Records deemed exempt under this section and disclosed to another entity continue to be exempt in the possession of the receiving entity."

Renumber accordingly

Written Testimony to the House Industry, Business, and Labor Committee

Senate Bill ~~2009~~ 2209

Andrew Alexis Varvel

March 4, 2019

Chairman Keiser and Members of the Committee:

My name is Andrew Alexis Varvel. I live in Bismarck, District 47.

North Dakota ought to remain an open records state.

So, please give SB 2009 a "**DO NOT PASS**" recommendation.

Thank you.

Andrew Alexis Varvel
2630 Commons Avenue
Bismarck, ND 58503
701-255-6639
mr.a.alexis.varvel@gmail.com

Attachment 2

Mar 13, 2019 SB 2209 Attachment 1

Anderson, Pamela K.

From: Seibel, Troy T.
Sent: Tuesday, March 5, 2019 11:20 AM
To: Anderson, Pamela K.
Subject: RE: Senate Bill 2209

Pam,

Here is the answer I got from our open records/meetings expert. Let me know if you have any additional questions or if I can help out....

In follow up to the committee hearing on SB 2209 – under open records law, the added records to be protected by 2209 would only be exempt from disclosure and would not be considered "confidential." The law differentiates between the two – exempt records may be protected and the public entity has the discretion on whether to release (see 44-04-17.1(5) (definition of "exempt record")) while confidential records can only be disclosed in accordance with law so a receiving entity may only get access to confidential information if there is a law specifically authorizing its release (see 44-04-17.1(3) (definition of "confidential record")). So the public entities, under SB 2209, have the discretion on whether to disclose the information – there may be certain entities/people that they want to share the information with and others they do not – and it would be up to them to make this determination.

There are certain laws in the Century Code that demand reporting of certain incidents. For example, NDCC chap. 51-30 requires that entities that own or licenses computerized data must disclose breach of security systems to those whose personal information may have been acquired by an unauthorized person. There is also a reporting mandate to the office of attorney general if the breach exceeds 250 individuals. SB 2209 would not prohibit this required disclosure – public entities would still need to report as required by law.

I hope this helps clarify the open records law as it applies to SB 2209.

Troy T. Seibel
Chief Deputy Attorney General
Office of Attorney General
600 E. Boulevard Ave., Dept. 125
Bismarck, ND 58505
701-328-2210
tseibel@nd.gov

From: Anderson, Pamela K. <pkanderson@nd.gov>
Sent: Monday, March 4, 2019 3:20 PM
To: Seibel, Troy T. <tseibel@nd.gov>
Subject: Senate Bill 2209

Troy, you are my go to person! So, here is a question for you. We had the hearing today on Senate Bill 2209 relating to open meeting and public records and utilities. We are in favor of the bill, but the question came up regarding the