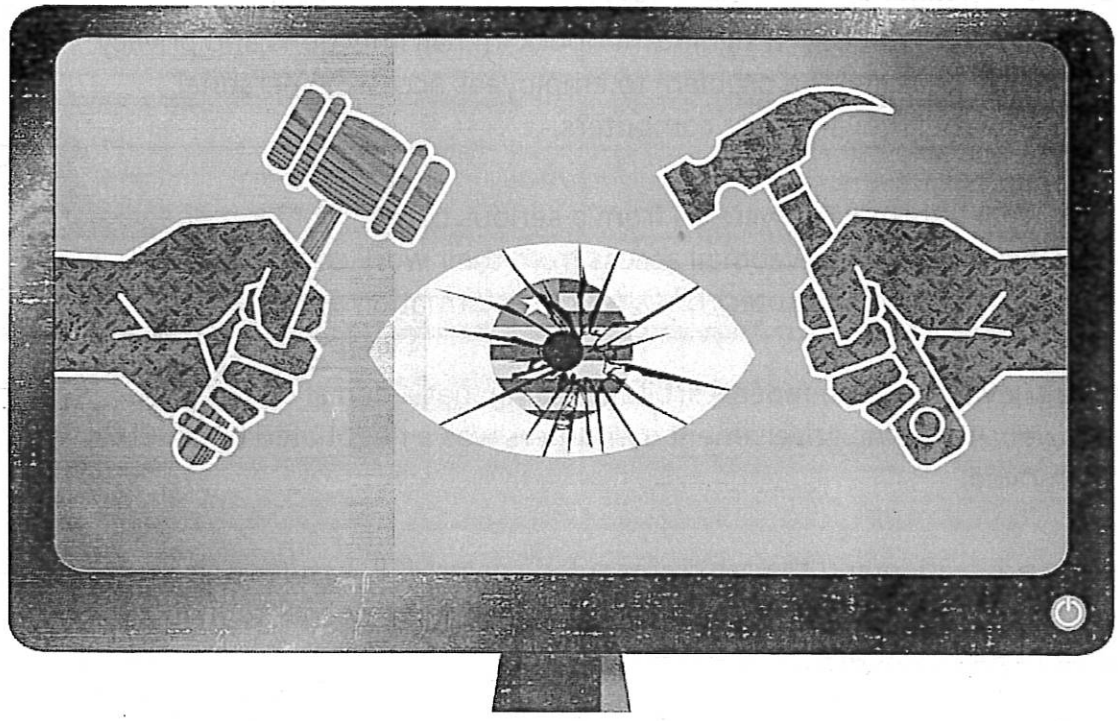
Palmer U.C. H.R. 5300 7-17-18

How collective bargaining undermines cybersecurity

Rules protecting federal unions make information breaches more likely



Threat to Federal Cybersecurity Illustration by Greg Groesch/The Washington Times more >

By Gary Palmer and Jason Chaffetz - - *Wednesday, February 24, 2016*

ANALYSIS/OPINION:

The federal government's most important responsibility is to protect this nation and its citizens. That includes protecting against cyberattacks.

Recall last summer's Office of Personnel Management (OPM) hack, when, in one of the largest data breaches in U.S. history, the personally identifiable information of more than 21.5 million Americans was stolen, including fingerprint data of nearly 6 million federal employees.

In light of such imminent dangers, federal agencies should have the full authority to act quickly to protect vital information systems. Mitigating a cyberthreat is a question of reacting within minutes and hours, not days.

Not so, says the American Federation of Government Employees (AFGE), the largest federal employee union.

A June 9, 2015 article in The Wall Street Journal revealed a major internal impediment to the ability of federal agency directors to protect agency information systems from a breach.

The article reported that in February 2011, the Immigration and Customs Enforcement Agency (ICE) noticed "a significant uptick in mail infections and privacy spills in its network." ICE traced the problem to employees accessing personal webmail accounts on their government computers.

In an effort to protect information systems from a serious breach, senior managers at ICE banned employees' personal webmail access from their work computers — a seemingly sensible safeguard to protect the agency's information systems.

Yet AFGE filed a grievance with a federal arbiter arguing that a denial of access at work to certain websites using government computers was a negotiated benefit that could not be removed.

The case went to arbitration and the arbitrator ruled against ICE, asserting that federal law did not give federal agencies "sole and exclusive discretion" to manage its information technology systems.

ICE appealed to the Federal Labor Relations Authority (FLRA), which also sided with the union.

In essence, the decision effectively established that the agency could not do anything to reduce security risks to its information systems without first providing the union with an opportunity to bargain.

In his dissent, authority member Patrick Pizzella astutely wrote, "Therefore, unlike my colleagues, I cannot conclude that Congress intended for our Statute to be read so expansively as to impose additional — in this case bargaining — requirements on federal agencies before they can act to secure the integrity of their federal [information technology] systems, the breach of which, could directly impact [o]ur nation's security and economic prosperity."

Mr. Pizzella further noted, "It is obvious to me (after having served for seven and a half years as the CIO at the U.S. Department of Labor) that neither the Authority nor the Arbitrator possesses the specialized knowledge or expertise that would permit us to decide when a federal agency ought to address specific security risks or permit us to second guess how that agency should exercise [its Federal Information Security Management Act] responsibilities."

Fast-forward to the staggering Office of Personnel Management breach announced in June 2015.

In July 2015, OPM attempted to block access from government computers to certain websites that they deemed security risks.

Yet once again, the union impeded this common-sense security measure and threatened a lawsuit, citing the Federal Labor Relations Authority opinion.

Never mind that shortly after the OPM breach was announced, the AFGE and the AFL-CIO sued the agency for failing to protect federal government employees' information.

The AFGE and AFL-CIO cannot have it both ways. It defies logic to insist agencies provide the opportunity to bargain before addressing cyberthreats, while simultaneously suing agencies for failing to protect employee information.

The current interpretation of the FLRA opinion is dangerous. If agency directors are obstructed from taking immediate action to protect employees' information without first going through collective bargaining, federal agencies are more vulnerable to attack.

Such an interpretation cannot stand. Putting collective bargaining rights above security is preposterous.

It is critical that Congress intervene and help make every effort to strengthen our cyberdefenses.

A good start is by ensuring that federal agency directors have the authority and flexibility they need to quickly deal with the continuing evolution of cybersecurity threats.

In the face of advanced persistent threats to cybersecurity, constraining federal agency directors with internal and external barriers leaves our government information systems unnecessarily exposed.

This creates a breach of our own making, a breach that the Congress can help close with thoughtful legislation.

• *Gary Palmer of Alabama and Jason Chaffetz of Utah are Republican members of the U.S. House of Representatives.*