

Are Protection and Control Engineers Provisioned with the Tools They Need to Combat Cyber-initiated Intrusions?

DENNIS K. HOLSTEIN , W. NEWTON , T.W. CEASE
CIGRE JWG B5-D2.46
USA

KEYWORDS

Cybersecurity, protection against cyber-initiated intrusions

1 INTRODUCTION

A mid-2012 survey on electric power utility cybersecurity policies related to the Protection and Control function was undertaken by Newton-Evans Research Company on behalf of CIGRE's B5-D2.46 Joint Working Group.

The findings of this report are based on a survey of 63 electric utilities around the world during the months of June, July and August 2012. Of these 63 utility responses, 25 were from the U.S. and Canada, while 38 were from other countries. The U.S. utilities included a mix of investor-owned (8), public power (7), and utility cooperatives (4).

This paper addresses several key questions and responses to assess the quality of technical, management and organizational provisions needed to prepare protection and control engineers with the tools to combat cyber-intrusions.

2 AWARENESS TRAINING

Awareness training tailored for protection and control engineers forms the foundation to combat cyber-intrusions that represent significant risk to the reliability and availability of power delivery.

Overall, there was a mostly even split between utilities that do offer cybersecurity training (35%), those that do not (33%), and those that don't currently but plan to by YE 2015 (32%). However, almost half of North American utilities indicated they currently offer cybersecurity training, while only one fourth of International utilities offer training now. The combination of current training and planned training is 65%, which is a good start but leaves a lot of room for improvement.

Training needs to be relevant to the work performed by protection and control engineers. If it is not relevant to their work, cybersecurity is significantly diminished. Overall, less than half of survey respondents tailor cybersecurity training to address job responsibility. However, in North America, 48% said they do this.

Most respondents seem to measure their cybersecurity training efforts as "average" to "inadequate", with fewer international utilities self-assessing their training as "adequate" or "complete". One fifth of North American utilities think their cybersecurity training is "very adequate". Very few responding officials (8%) think their cybersecurity training is "fine as it is." North American utilities see room for "some improvement" while Internationals responded that "Yes, a lot" of improvement could be made.

Forty-four percent of North American utilities said their P&C system personnel have signed acceptable use policies, and 30% of International utilities reported the same. Five out of the eight North American investor-owned utilities responding to this one inquiry answered "Yes."

Nearly one half of all utilities surveyed DO monitor personnel access to P&C system components. Almost one quarter of respondent do not currently monitor, but plan to by year end 2015.

It is clear from these responses that significant structural improvements are needed to improve EPU's awareness training programs.

3 INCIDENT RESPONSE

Forty-two percent of North American utilities and twenty-one percent of International Utilities reported having an incident response plan for their P&C system.

More than one half of the sample of utilities in North America reported that they have adequate controls in place to monitor their P&C system for security incidents, Another 24% said even though they don't have such controls currently, they will have these in place by year end 2015. Only 1 in 4 International utilities in the sample think they have adequate security incident monitoring controls in place.

About one half of utilities across the sample do not benchmark or keep a scorecard of P&C cybersecurity incidents. Thirty percent of international utilities and twenty percent of North American utilities in the sample are planning to do so by the end of 2015. Only seven out of all 60-plus utilities in the sample reported using a scorecard for P&C cybersecurity incidents. Out of those seven, two said the scorecard is automated.

Given the heightened awareness to security issues, the need to protect critical EPU infrastructures, and government funding in North America and the European Union the lack of benchmarking P&C security incidents is a surprise. It is difficult to understand how EPUs can manage effective cybersecurity programs without properly monitoring and benchmarking incidents.

4 QUALIFYING SECURITY PATCHES

Overall, roughly one third of utilities test patches, one third do not and almost a third currently do not, but plan to do so by year end 2015.

Even though nearly two-thirds of the responding EPUs plan to test security patches by the end of 2015, the fact remains that one-third have no plans to do so. Unfortunately, the survey did not ask additional questions to better understand the patching issues and constraints. This is a subject that needs further investigation.

5 EPU SHORTLIST OF SOLUTIONS NEEDED

Fifty-one out of all sixty-three survey respondents provided written feedback on the question "What is your short list of cybersecurity solutions needed to protect your P&C systems?" Responses were sorted into types based on a combination of word usage and implied meaning. Although all of the written feedback expressed valid concerns and cybersecurity solutions, about half of the written responses were too unique and varied to be categorized (all responses are listed by respondent number over the next few pages.)

More than half of the respondents (55%) indicated the need to restrict access and connectivity through a number of means: network separation/segmentation, access control, closed networks, no internet connectivity, restricting physical access, or limiting the number of access points in general (physical or electronic.) Thirty-seven percent mentioned some method of access logging or network monitoring such as IDS (intrusion detection system). Only 4% mentioned encryption, which is obviously further down the "short list" of cybersecurity needs.

Similar to this question, many respondents (12) mentioned some variant of "restrict or control access and connectivity" as the preferred cybersecurity solution. There were 4 mentions for firewall software and 1 for antivirus software, but 4 respondents also commented that there is no *single* preferred solution for cybersecurity – that they are either all equally important, or there are multiple preferred solutions.

6 USE OF PERSONAL DEVICES

More than three fourths of respondents DO NOT allow their employees to use personal devices for either P&C maintenance or for configuring P&C components.

Out of forty-eight utilities who do not allow their employees to use personal devices for either P&C maintenance or components, only two are planning to allow this for P&C maintenance and one utility plans to allow the use of personal devices for configuring P&C components.

About one-fifth of all respondents indicated they allow third-party support to use their own personal devices for P&C maintenance, and almost one-fourth allow them to use personal devices for configuring components.

Seven percent of respondents overall said they do provide support to programs loaded on third party support technician's personal devices for P&C maintenance, and 11% said they support such programs for configuring components. Support for both of these is a bit higher internationally than for North American utilities.

Fifty-five percent of all responding utilities estimate that none of their third party technicians use personal devices for P&C maintenance. Nineteen percent weren't sure, and eighteen percent said about one-fourth of the third party technicians they hire use personal devices for P&C maintenance. Restricting the use of personal devices is somewhat confusing. EPU's clearly discourage the use of personal devices by their employees, but they don't seem to impose the same restrictions on third party technicians.

7 IMPACT OF REGULATORY REQUIREMENTS

North American utility P&C cybersecurity policies are more driven by regulatory requirements than was reported among international utilities. Eighty-nine percent of international utilities answered "NO" to this question, while only 40% of North American utilities answered "NO."

Many North American utilities cited NERC and FERC requirements as being applicable or influential on their P&C cybersecurity policies. One international utility mentioned ISO security standards.

The bulk of the input for this question came from the 32 international utilities, as well as 10 North American utilities, that answered "NO" (that is, not driven by regulatory mandates) to the question "Are your P&C cybersecurity policies and procedures derived from regulatory requirements?"

IT department guidelines exert the most influence on cybersecurity policies, followed by industry guidelines and utility guidelines. Professional associations seem to have more influence on international cybersecurity policies than in North America.

8 CONCLUSIONS

CIGRE JWG B5-D2.46 is using this survey and analysis of responses to guide the development of a technical brochure titled "Application and management of cybersecurity measures for protection and control systems." To supplement the response to the survey JWG members are presenting papers in venues such as this one to solicit additional opinions and interpretation of the questions. These opinions and interpretations will also be used to improve the technical brochure.

There are several important conclusions that can be drawn from the results to-date.

1. Given the heightened security awareness and funding within North America and the European Union, response from EPU's is disappointing. The lack of automated tools for benchmarking security incidents is most troublesome because it degrades effective management of security policies.
2. Although EPU's are implementing security awareness training there is room for improvement. Most notably, the training should be closely coupled to the job responsibility to improve relevance and acceptance of security responsibilities.
3. Security patch management is at best poorly implemented. IEC/TR 62443-2-3 will be issued for review in early 2013. ISA99's goal is to eventually publish this draft technical report as a technical specification or standard. EPU's are encouraged to review and comment on part 2-3 to improve its relevance to their organizational environments and operating constraints.
4. There is such a strong business case and cost saving for the use of personal devices that eventually EPU's will have to lift their restrictions on how those devices is qualified for use on P&C networks and devices. This is true of their use for remote access as well as local access within the substations.